CA/251/H63

Miami University Libraries

# REPRESENTATION THEORY OF LIE ALGEBRAS

by

G. Hochschild

Notes by G. Leger

The University of Chicago

Summer 1959

# REPRESENTATION THEORY OF LIE ALGEBRAS

by

G. Hochschild

Notes by G. Leger.

The University of Chicago

Summer 1959

QA
251
H63

# PART I

## GENERAL REPRESENTATION THEORY OF LIE ALGEBRAS

### 1. Universal Enveloping Algebra.

Def. Let $K$ be a commutative ring with 1. A Lie algebra over $K$ is a $K$-module $L$ together with a bilinear map of $L \times L \longrightarrow L$ (denoted by $(x,y) \longrightarrow [x,y]$) such that

(i) $[x,x] = 0$

(ii) $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$ for all $x,y,z$ in $L$.

(ii) is known as the Jacobi identity.

Let $T$ denote the tensor algebra over the $K$-module of $L$ and let $I$ denote the two-sided ideal of $T$ generated by all elements of the form $x \otimes y - y \otimes x - [x,y]$ with $x$, $y$ in $L$. The factor algebra $U = T/I$ is called the universal enveloping algebra of $L$.

Let $M$ be a unitary $K$-module and let $E(M)$ be the $K$-algebra consisting of all $K$-endomorphisms of $M$. An -module structure on $M$ is a linear map $\rho$: $L \longrightarrow E(M)$ such that $\rho[x,y] = \rho(x)\rho(y) - \rho(y)\rho(x)$ for all $x,y$ in $L$. When $\rho$ is extended in the canonical fashion to a unitary $K$-algebra homomorphism of $T$ into $E(M)$ (still denoted by $\rho$) we shall evidently have $\rho(I) = (0)$. Hence $\rho$ induces a unitary homomorphism of $U$ into $E(M)$, i.e. $M$ now has the structure of a unitary $U$-module. It is clear from the definition of $U$ that we obtain in this fashion a one-to-one correspondence between $L$-module structures and unitary $U$-module structures. (The importance of the universal enveloping algebra lies in this fact.)

If M is any L-module or U-module, $m \in M$ and $x \in L$ or U, we shall denote by x.m the transform of m under the endomorphism of M corresponding to x.

Theorem 1. Suppose L is free over K and let $(x_i)$ be a simply ordered free K-basis of L. Let $u_i$ be the canonical image of $x_i$ in U. Then 1 and the ordered monomials

$$u_{i_1} \cdots u_{i_n} \quad \text{with} \quad i_1 \leq \cdots \leq i_n$$

constitute a free K-basis for U.

Proof: (Iwasawa, Cartan-Eilenberg) It is easy to see (by an evident "straightening" procedure) that the ordered monomials, including the empty monomial 1, span U over K so that it suffices to show that they are free over K. In order to see this, we shall define the structure of an L-module (and hence that of a U-module) on the symmetric K-algebra S built over L. S is the factor algebra of T by the ideal generated by the elements $x \otimes y - y \otimes x$ with $x, y \in L$.

We may identify S with the algebra of ordinary commutative polynomials in the basis elements $x_i$ with coefficients in K. Thus we identify L with its canonical image in S. Denote by $S_p$ the submodule of S consisting of all polynomials of degree $\leq p$. If $J = (j_1, \ldots, j_n)$ is any set of indices, we shall abbreviate $x_{j_1} \cdots x_{j_n}$ by $x_J$. We write $j \leq J$ to mean $j \leq j_p$ for all $j_p$ in J. We shall define an L-module structure on S such that

(1) If $j \leq J$ then $x_j . x_J = x_j x_j$

(2) If $x \in L$ and $s \in S_q$ then $x.s - xs \in S_q$.

The definition will be made inductively on q. For $q = 0$ the operation of L on $S_o = K$ is forced by (1); in fact, the operation

of $x \in L$ is simply multiplication by $x$ so that (2) is trivially satisfied. Now suppose that the operation of $L$ on $S_q$ has already been defined for some $q$ so as to satisfy conditions (1) and (2) and also such that the commutator conditions

$$x.(y.s) - y.(x.s) = [x,y].s$$

are satisfied for all $x$, $y$ in $L$ and all $s$ in $S_{q-1}$. We must define the transforms $x_j.x_J$ for $x_J \in S_{q+1}$. If $j \leq J$ we define

$$x_j.x_J = x_jx_J \quad \text{so as to satisfy (1) and (2).}$$

If $j \not\leq J$ we can write, uniquely, $J = (k, J_1)$ with $k \leq J_1$. Then $j > k$. By the inductive hypothesis we have

$$x_j.x_{J_1} - x_jx_{J_1} \in S_q$$

so that $x_k.(x_j.x_{J_1} - x_jx_{J_1})$ is defined. We put (forcing in the commutator condition)

$$x_j.x_J = [x_j,x_k].x_{J_1} + x_k.(x_j.x_{J_1} - x_jx_{J_1}) + x_kx_jx_{J_1}$$

then condition (2) is evidently satisfied.

Also, these definitions evidently give

$$x_r.(x_s.x_Q) - x_s.(x_r.x_Q) = [x_r,x_s].x_Q$$

whenever $r > s \leq Q$ and $x_Q \in S_q$. Since each side is antisymmetric, this holds also if $s > r \leq Q$. It holds trivially if $r = s$. Hence, there only remains to prove this if both $r \not\leq Q$ and $s \not\leq Q$. Then we can write, uniquely, $Q = (h, Q_1)$ with $h \leq Q_1$ and we have $r > h$ and $s > h$.

Now, by the induction hypothesis,

$$x_s.x_Q = x_s.(x_n.x_{Q_1}) = x_h.(x_s.x_{Q_1}) + [x_s, x_h].x_{Q_1}$$

$$= x_h.(x_sx_{Q_1}) + x_h.(x_s.x_{Q_1} - x_sx_{Q_1}) + [x_s,x_h].x_{Q_1} \quad .$$

Hence

$$x_r\cdot(x_s\cdot x_Q) = x_r\cdot(x_h\cdot(x_s x_{Q_1})) + x_r\cdot(x_h\cdot(x_s\cdot x_{Q_1} - x_s x_{Q_1})) + x_r\cdot([x_s,x_h]\cdot x_{Q_1}).$$

By the inductive hypothesis we may apply the commutator condition to the last two terms. Since $r > h \leq (s, Q_1)$ we may also apply the commutator condition to the first term. Thus we obtain

$$\begin{aligned} x_r\cdot(x_s\cdot x_Q) &= x_h\cdot(x_r\cdot(x_s x_{Q_1})) + [x_r,x_h]\cdot(x_s x_{Q_1}) + x_h\cdot(x_r\cdot(x_s\cdot x_{Q_1} - x_s x_{Q_1})) \\ &+ [x_r,x_h]\cdot(x_s\cdot x_{Q_1} - x_s x_{Q_1}) + [x_s,x_h]\cdot(x_r\cdot x_{Q_1}) \\ &+ [x_r,[x_s,x_n]]\cdot x_{Q_1} \\ &= x_h\cdot(x_r\cdot(x_s\cdot x_{Q_1})) + [x_r,x_h]\cdot(x_s\cdot x_{Q_1}) + [x_s,x_h]\cdot(x_r\cdot x_{Q_1}) \\ &+ [x_r,[x_s,x_h]]\cdot x_{Q_1} . \end{aligned}$$

Now interchange r and s and subtract the result. Then we obtain

$$x_r\cdot(x_s\cdot x_Q) - x_s\cdot(x_r\cdot x_Q) = x_h\cdot(x_r\cdot(x_s\cdot x_{Q_1}) - x_s\cdot(x_r\cdot x_{Q_1})) + [x_r,[x_s,x_h]]\cdot x_{Q_1} - [x_s,[x_r,x_h]]\cdot x_{Q_1} .$$

Using the induction hypothesis for the first term on the right side and the Jacobi identity for the remaining two terms we find

$$x_r\cdot(x_s\cdot x_Q) - x_s\cdot(x_r\cdot x_Q) = x_h\cdot([x_r,x_s]\cdot x_{Q_1}) - [x_h\cdot[x_r,x_s]]\cdot x_{Q_1} ,$$

so that by the induction hypothesis the right side is

$$[x_r, x_s]\cdot(x_h\cdot x_{Q_1}) = [x_r,x_s]\cdot x_Q .$$

Thus the commutator condition is satisfied in all cases and our

induction is completed. Thus $S$ has an $L$-module structure satisfying condition (1). Now consider the corresponding $U$-module structure of $S$. Under this structure, the transform of the identity element $1$ of $S$ by the ordered monomial $u_{i_1} \cdots u_{i_n}$, $i_1 \leqq \cdots \leqq i_n$, is $x_{i_1} \cdots x_{i_n}$ by virtue of condition (1). Since the set of elements consisting of $1$ and $x_{i_1} \cdots x_{i_n}$, $i_1 \leqq \cdots \leqq i_n$, is $K$-free in $S$, it follows that the set consisting of $1$ and the ordered monomials $u_{i_1} \cdots u_{i_n}$ is $K$-free in $U$. This completes the proof of Theorem 1.

Notation: $T_n = \sum_{i \leqq n} T^i$ ; $U_n$ denotes the $K$-submodule of $U$ which is the canonical image of $T_n$ in $U$. This leads us to an increasing filtration of $U$, i.e., $U_n \subset U_{n+1}$

$$\bigcup_{n=0}^{\infty} U_n = U \quad \text{and} \quad U_n U_m \subset U_{n+m} \ .$$

With this filtration is associated a graded association algebra $G$ defined by

$$G = \sum \oplus G^n \quad \text{where} \quad G^n = U_n/U_{n-1} \ , \quad U_{-1} = 0$$

and $\sum \oplus$ indicates direct $K$-module sum. The multiplication on $G$ is the one induced by that of $U$ and has the property $G^n G^m \subset G^{n+m}$. An ideal $J$ of $G$ is called homogeneous if $J = \sum \oplus J \cap G^n$ .

Theorem 1 evidently implies that if $L$ if free over $K$, $G$ is canonically isomorphic with $S$.

Lemma 1. Let $U$ be an increasingly filtered ring and suppose that its associated graded ring satisfies the maximal condition for left (right) ideals. Then $U$ satisfies the maximal condition for left (right) ideals.

Proof: For $u \in U$, let $[u]$ be the smallest index $n$ such that $u \in U_n$ and let $\bar{u}$ denote the canonical image of $U$ in $U_{[u]}/U_{[u]-1}$. Then if $u, v \in U$,

$$\overline{uv} = \begin{cases} \overline{uv} & \text{if } uv \notin U_{[u]+[v]-1} \\ 0 & \text{if } uv \in U_{[u]+[v]-1} \end{cases}.$$

If $J$ is any left (right) ideal in $U$, we denote by $\bar{J}$ the set of all finite sums $\sum_{j \in J} \bar{j}$ in $G$. Then, because of the above, $\bar{J}$ is a homogeneous left (right) ideal in $G$.

Now let $S$ be any set of left (right) ideals $J$ of $U$. Choose $J_1 \in S$ such that $\bar{J}_1$ is maximal in the set of $\bar{J}$ with $J \in S$. Suppose $J \in S$, $J \supset J_1$. If $J \neq J_1$, choose $j \in J$ such that $j \notin J_1$ and such that $[j]$ is minimal. Clearly $\bar{J} = \bar{J}_1$ so that $\bar{j} = \sum_p \bar{u}_p$ with $u_p \in J_1$ and $[u_p] = [j]$. Then $j - \sum_p u_p \in U_{[j]-1} \cap J$. But $j - \sum_p u_p \notin J_1$ and this contradicts the minimality of $[j]$. Thus $J = J_1$ so that $J_1$ is maximal in $S$. Q.E.D.

By the remark immediately preceding Lemma 1 we have

Corollary. Suppose $L$ is a Lie algebra of finite dimension over a field $K$. Then $U$ satisfies the maximal condition for left and right ideals.

Lemma 2. Let $K$ be any commutative ring with 1 and $U$ a $K$-algebra with 1. Let $A$, $B$ be left ideals of $U$ such that $U/A$ and $U/B$ are finitely generated $K$-modules and suppose $B$ is finitely generated as a $U$-module. Then $U/AB$ is a finitely generated $K$-module.

Proof: Let $u_1, \ldots, u_p \in U$ be such that $u_1 + A, \ldots, u_p + A$ span $U/A$ over $K$ and $v_1, \ldots, v_q \in U$ be such that $v_1 + B, \ldots, v_q + B$

span $U/B$ over $K$ and let $b_1, \ldots, b_r$ span $B$ over $U$. Then

$$U = Kv_1 + \ldots + Kv_q + B$$

$$= Kv_1 + \ldots + Kv_q + Ub_1 + \ldots + Ub_r$$

$$= Kv_1 + \ldots + Kv_q + (Ku_1 + \ldots + Ku_p)b_1 + \ldots + (Ku_1 + \ldots + Ku_p)b_r + A$$

so that the cosets of $v_1, \ldots, v_q$ and $u_1b_1, \ldots, u_pb_r$ span $U/AB$ over $K$.

Notation: If $V$ is a vector space over a field $K$ and $S$ is a subspace of $V$ then codim $S$ (codimension) is the dimension of $V/S$ over $K$.

Now from Corollary 1 and Lemma 1 and 2 we have

Theorem 2. Let $L$ be a Lie algebra of finite dimension over the field $K$ and let $U$ be the universal enveloping algebra of $L$. Then $U$ satisfies the maximal condition for left (right) ideals. Further, if $A$ and $B$ are left (right) ideals of finite codimension then $AB$ also has finite codimension.

## 2. Nilpotency and Solvability.

Notation: If $A$ is an associative algebra over a field $K$ and if $S$ and $T$ are subspaces of $A$, then $[S,T]$ denotes the subspace of $A$ spanned by the elements $st - ts$ for all $s \in S$, $t \in T$.

If $x$ is an element of $A$ such that $x^n = 0$ for some integer $n$ then $x$ is called nilpotent; an ideal $J$ is called nilpotent if $J^k = (0)$ for some integer $k > 0$. Hence if $A$ is a finite dimensional associative algebra over $K$ then the sum of all nilpotent left ideals of $A$ is a nilpotent left ideal containing every nilpotent ideal. This is called the radical of $A$.

Lemma 3. Let $A$ be a finite dimensional associative algebra over a field $K$ of characteristic 0 and let $R$ be the radical of $A$. Let $S$ be a subspace of $A$. Then if $z \in [S,A]$ is such that $[(z), A] \subset R$, $z$ is nilpotent.

Proof: We have $z(sa - as) = [z,s]a + (sza - zas)$ for all $a \in A$, $s \in S$. Thus $z[S,A] \subset [S,A] + R$ and, by induction on $k$, we see that $z^k \in [s,A] + R$ for every $k > 0$. For $c \in A$, we denote by $T_A(c)$ the trace of the endomorphism of $A$ consisting in left multiplication by $c$. Then $T_A(z^k) = 0$ for all $k > 0$ since the trace of commutators and nilpotent elements is 0.

There is a positive integer $n$ such that $z^n A = z^{n+1} A$ and we let $B$ be the subspace of all $a \in A$ such that $z^k a = 0$ for some $k$. Then $A$ is the $K$-direct sum of $z^n A$ and $B$ and further, $z^n A$ and $B$ are stable under left multiplication by $z$. Thus

$$T_A(z^k) = T_{z^n A}(z^k) + T_B(z^k) \qquad \text{for all } k > 0 .$$

But $z$ is nilpotent on $B$ so that

$$T_Z(z^k) = T_{z^n A}(z^k) \qquad \text{for all } k > 0 .$$

Let $\xi$ be the left multiplication by $z$ on $z^n A$ and let $t^m + c_1 t^{m-1} + \ldots + c_0$ be the minimular polynomial of $\xi$. Since $\xi$ is an automorphism of $z^n A$, $c_0 \neq 0$. Now we have

$$0 = T(\xi^m + \ldots + c_0) = T_{z^n A}(z^m + \ldots + c_0)$$
$$= c_0 \dim (z^n A) .$$

Hence $z^n A = 0$ which means that $z$ is nilpotent on $Z$ and hence nilpotent.

Def. Let K be a field of characteristic 0. If M is an R-module where R is any K-algebra, then M is called semi-simple if every R-submodule of M is a direct R-module summand of M.

Def. Let L be a Lie algebra. The center of L =

$$= \{ x \in L \mid [x,y] = 0 \text{ for all } y \in L \} .$$

Theorem 3. Let L be a Lie algebra of linear transformations of a finite dimensional vector space V over a field K of characteristic 0. Suppose that V is semi-simple as an L-module and let C be the center of L. Then $[L,L] \cap C = (0)$, L/C has no abelian ideal, and every element of C is a semi-simple linear transformation.

Proof: Let A be the associative algebra of linear transformations of V that is generated by L and the identity transformation. Then V is semi-simple as an A-module. It follows that A has no non-zero nilpotent left ideal. (Otherwise A has a left ideal $B \neq 0$ such that $B^2 = 0$. Then B.V is an A-submodule of V and hence $V = B.V \oplus W$ where W is an A-submodule. Clearly $B.W \subset B.V \cap W = (0)$. Thus $B.V = B^2V + B.W = (0)$ so that $B = (0)$.)

Let Z be the center of A. Then $C \subset Z$ and, moreover, Z has no non-zero nilpotent elements. It follows that the associative algebra generated by an element c in C is a direct sum of fields. Hence c is a semi-simple linear transformation.

$A([A,A] \cap Z) \subset [A,A] \cap Z$ so that $[A,A] \cap Z$ is a subalgebra of A. By Lemma 3, every element of $[A,A] \cap Z$ is nilpotent. Hence $[A,A] \cap Z = (0)$ and a fortiori, $[A,A] \cap C = (0)$.

Let $J$ be an ideal of $L$ such that $[J,J] \subset C$. Then $[J,J] \subset [L,L] \cap C$ so that $[J,J] = (0)$, whence $[L,J]$ is abelian. By applying Lemma 3 (with $S = J$) we see that every element of $[L,J]$ is nilpotent. Hence it follows that the associative algebra $B$ generated by $[L,J]$ is nilpotent. Since $[L,J]$ is an ideal in $L$, $AB \subset BA + B$. (In fact it suffices to show that for $a \in L$, $aB \subset Ba + B$ and this is seen by writing the elements of $B$ as polynomials in the elements of $[L,J]$.) By induction on $k$, $(AB)^k \subset B^kA + B^k$ for all $k > 0$ whence $AB$ is a nilpotent ideal of $A$. Thus $AB = (0)$ so that $B = (0)$, i.e., $J \subset C$. Q.E.D.

Define $L_1 = L$, $L_2 = [L,L]$, ..., $L_{i+1} = [L_i, L_i]$. $L$ is called <u>solvable</u> if $L_n = 0$ for some $n$. Note that if $L_{n-1} \neq (0)$, $L_n = (0)$, then $L_{n-1}$ is a non-zero abelian ideal of $L$.

<u>Theorem 4.</u> (Lie). Let $L$ be a solvable Lie algebra over a field of characteristic 0. Then every finite dimensional, semi-simple $L$-module is annihilated by $[L, L]$.

<u>Proof:</u> Let $M$ be such a module; then the image $\bar{L}$ of $L$ in the algebra of K-endomorphisms of $M$ is a solvable Lie algebra of linear transformations of $M$. Let $\bar{C}$ denote the center of $\bar{L}$. Then, since $\bar{L}$ is solvable, so is $\bar{L}/\bar{C}$. By Theorem 3 $\bar{L}/\bar{C}$ has no abelian ideals whence $\bar{L}/\bar{C} = (0)$, i.e. $\bar{L} = \bar{C}$. Thus $(0) = [\bar{L}, \bar{L}].M = (L,L].M$. Q.E.D.

<u>Def.</u> Let $L$ be a Lie algebra and $M$ and $L$-module. We say that a subset $S$ of $L$ is <u>nilpotent on $M$</u> if $S^n.M = (0)$ for some $n > 0$.

<u>Lemma 4.</u> Let $M$ be an $L$-module, $S$ a subspace of $L$ which is nilpotent on $M$. Let $x \in L$ be such that $[x,S] \subseteq A$ and $x$ is nilpotent on $M$. Then the subspace spanned by $x$ and $S$ is nilpotent on $M$.

Proof: There exist integers $p$ and $q$ such that $S^p.M = (0)$, $x^q.M = (0)$. We claim that $((x)+S)^{pq}.M = (0)$. Consider (in the universal enveloping algebra of L) a monomial $u_1 \cdots u_{pq}$ where each $u_i$ is either $\in S$ or $= x$. For $s \in S$, $sx = xs + [s,x]$. Hence $u_1 \cdots u_{pq}$ can be written as a sum of monomials of the form $x^r S^t$ where $r = 0,1, \ldots$ and $t$ is the number of indices $i$ for which $u_i \in S$. Hence $u_1 \cdots u_{pq}.M = 0$ unless $t < p$. But if $t < p$, there must be an index $i$ such that $u_{i+1}, \ldots, u_{i+q}$ are all equal to $x$ because there are $pq - t > p(q-1)$ elements $x$ in the $t + 1 \leq p$ intervals not containing elements of $S$. Thus we have again $u_1 \cdots u_{pq}.M = (0)$.

Theorem 4. (Engel). Let $L$ be a Lie algebra over a field $K$ and let $M$ be an L-module of finite dimension over $K$. Suppose that every element of $L$ is nilpotent on $M$. Then $L$ is nilpotent on $M$.

Proof: For $x \in L$ we denote by $D_x$ the linear endomorphism (actually a derivation by the Jacobi identity) defined by $D_x(y) = [x,y]$. Let $L'$ be the image of $L$ in the endomorphism algebra of $M$. Then for every $x' \in L'$, $D_{x'}$ is nilpotent. In fact, $D^m_{x'}(y')$ is a sum of terms $(x')^p y' (x')^q$ whence $D^m_{x'} = 0$ for sufficiently large $m$. Hence, replacing $L$ be $L'$ if necessary, we may assume that $L$ is finite dimensional and that $D_x$ is nilpotent for every $x \in L$.

We proceed by induction on the dimension of $L$. Let $H$ be a subalgebra of $L$ having the largest possible dimension. By the induction hypothesis, $H$ is nilpotent on $L$ (where the endomorphism of $L$ corresponding to an element $x \in H$ is $D_x$). It follows that there is an element $y \in L$ such that $y \notin H$ but $[H,y] \subset H$. Now since $H$ and $y$ are nilpotent on $M$ it follows from Lemma 4 that $H + (y)$ is nilpotent on $M$. Also, $H + (y)$ is a subalgebra of $L$ and must therefore coincide with $L$ by the maximality of $H$. Thus $L$ is nilpotent on $M$. Q.E.D.

Theorem 5. (Cartan). Let $L$ be a Lie algebra of linear transformations of a finite dimensional vector space $V$ over a field of characteristic 0. Suppose $T(\overline{xy}) = 0$ for all $x,y \in L$ ($T(x)$ = trace $x$). Then $L$ is solvable.

Proof: We may assume that $K$ is algebraically closed. To see this, let $\overline{K}$ be the algebraic closure of $K$ and let $\overline{L} = L \otimes_K \overline{K}$ operate on $V \otimes_K \overline{K}$ in the obvious way. Then $T(\overline{xy}) = 0$ for all $\overline{x}, \overline{y} \in \overline{L}$. Now note that if $\overline{L}$ is solvable, $L$ is solvable.

We proceed by induction on the dimension of $L$. The theorem is trivial if this dimension is 0 or 1, and we choose a proper subalgebra $H$ of maximal dimension. Then $H$ is solvable by the induction hypothesis.

Consider the $H$-module whose underlying space is that of $L/H$. Let $M$ be an $H$-submodule of $L/H$ of minimal possible dimension. Then $M$ is a simple $H$-module and this, by Theorem 4, $[H, H].M = (0)$. Applying Schuer's Lemma we see that every element of $H$ operates on $M$ as a scalar multiple of the identity whence $M$ is one dimensional. Hence the inverse image of $M$ in $L$ has the form $H + (y)$ and further, is a subalgebra of $L$. But $H$ was maximal so that $H + (y) = L$.

There is a linear functional $\mu$ on $H$ such that $[x,y] - \mu(x)y \in H$ for all $x \in H$.

Let $W$ be any non-zero simple $L$ module and let $W_o$ be a non-zero simple $H$-submodule; $W_o = Ke_o$. Put $e_{i+1} = y.e_i$ for $i \geq 0$ and set $W_j = Ke_o + Ke_1 + \ldots + Ke_j$. For $x \in H$,

$$\begin{aligned} x.e_{i+1} &= x.(y.e_i) = y.(x.e_i) + [x,y].e_i \\ &= y.\left\{(x.e_i) + \mu(x)e_i\right\} + x'.e_i \end{aligned}$$

with $x' \in H$.

Hence we see by induction on $j$ that each $W_j$ is H-stable. Let $x.e_o = \lambda(x)e_o$ for all $x \in H$. We claim that for every $x \in H$ and every $j$,

$$x.e_j - (\lambda(x) + j\mu(x))e_j \in W_{j-1} \ , \ (W_{-1} = (0)).$$

Now for $j = 0$ this is clear. Suppose this true for $i$. Then

$$\begin{aligned} x.e_{i+1} - (\lambda(x) + (i+1)\mu(x))e_{i+1} \\ &= y.[x.e_i + \mu(x)e_i - (\lambda(x) + (i+1)\mu(x))e_i] + x'.e_i \\ &= y.[x.e_i - (\lambda(x) + i\mu(x))e_i] + x'.e_i \\ &\in y.W_{i-1} + W_i \subset W_i \ . \end{aligned}$$

Let $q$ be the largest $i$ such that $e_o, \ldots, e_i$ are linearly independent. Then $W_q$ is an L-submodule of $W$. But $W$ is simple so that $W_q = W$. Hence, for $x \in H$,

$$T_W(x) = (q+1)\ \lambda(x) + \frac{q(q+1)}{2}\ \mu(x).$$

We may assume $L = [L,L]$ since otherwise the theorem follows from the induction hypothesis. Therefore every element of $H$ is a sum of commutators so that $T_W(x) = 0$ whence $\lambda(x) = -\frac{q}{2}\ \mu(x)$. Hence

$$x.e_j - (j - \tfrac{q}{2})\ \mu(x)\ e_j \in W_{j-1}$$

for all $x \in H$ and all $0 \leq j \leq q$, and

$$T_W(x^2) = \sum_0^q (j - \tfrac{q}{2})^2\ \mu(x)^2$$

(for any simple L-module $W$).

Let $V = V_0 \supset V_1 \supset \cdots \supset V_k = (0)$ be a composition series for the L-module V. Applying the above result to the simple L-modules $V_i/V_{i+1}$ we obtain

$$T_V(x^2) = \sum_{i=0}^{k-1} \sum_{j=0}^{q_i} (j - \frac{1}{2} q_j)^2 \mu(x)^2$$

where $q_i = \dim(V_i/V_{i+1}) - 1$. If $\mu(x) = 0$ for all $x \in H$, then $[L,L] \subset H$ contrary to our assumption that $[L,L] = L$. Thus $\mu(x) \neq 0$. Therefore

$$\sum_{i=0}^{k-1} \sum_{j=0}^{q_i} (j - \frac{1}{2} q_i)^2 = 0$$

whence each $q_i = 0$. This means that each $V_i/V_{i+1}$ is one dimensional. Since $L = [L,L]$, $T_V(u) = 0$ for all $u \in L$ whence L annihilates each $V_i/V_{i+1}$, i.e., $L.V_i \subset V_{i+1}$. Hence if $u_1, \ldots, u_n \in L$, then $u_1 \ldots u_k.V = 0$, i.e., $u_1 \ldots u_k = 0$. Hence L is solvable. Q.E.D.

3. Semi-simplicity.

Henceforth the basic fields for the Lie algebras and vector spaces we discuss will be implicitly assumed to be of characteristic 0.

Def. A Lie algebra is called semi-simple if it has no non-zero abelian ideal.

Remark: It is clear that L is semi-simple if and only if L has no non-zero solvable ideal.

Def. An L-module M is called semi-simple if, for every submodule N of M there is a submodule Q with

$$M = N + Q, \quad N \cap Q = (0).$$

If $S$ is a representation of $L$, we define the trace form $f_\rho$ of $\rho$ by

$$f_\rho(x,y) = T(\rho(x)\rho(y)).$$

Then, as is easily verified by direcy computation

$$\underline{f_\rho([x,y], z) = f_\rho(x,[y,z])} \quad .$$

Theorem 6. Let $L$ be a semi-simple, finite dimensional Lie algebra. Let $\rho$ be a faithful (i.e. kernel of $\rho = 0$) finite dimensional representation of $L$. Then the trace form $f_\rho$ is non-degenerate. If the trace form of the adjoint representation is non-degenerate, $L$ is semi-simple.

Proof: Let $H$ be the set of all $x$ in $L$ such that $f_\rho(x,y) = 0$ for every $y$ in $L$. By the remark before the theorem, $H$ is an ideal in $L$. Theorem 5, applied to $\rho(H)$, yields that $H$ is solvable. Since $L$ is semi-simple, it follows that $H = 0$. Therefore, $f_\rho$ is non-degenerate.

Now suppose that the trace form for the adjoint representation of a Lie algebra $L$ is non-degenerate. Let $A$ be an abelian ideal of $L$. Take $x$ in $A$, $y$ in $L$ and consider $D_xD_y$. This maps $L$ into $A$ and $A$ into $(0)$, so that $T(D_xD_y) = 0$. Since this holds for all $y \in L$, it follows that $x = 0$. Thus $A = (0)$.

Theorem 7. If $L$ is semi-simple then the adjoint representation of $L$ is semi-simple and $L = [L,L]$.

Proof: Since $L$ is semi-simple, its center is $(0)$ whence its adjoint representation is faithful. Hence, by Theorem 6, its trace form is

non-degenerate. Let $I$ be any ideal of $L$ and let $J$ be the set of all $x \in L$ for which $T(D_x D_y) = 0$ for all $y \in I$. $J$ is an ideal of $L$ and $I \cap J$ is solvable (by Theorem 5) and hence is (0). As a subspace of $L$, $J$ is defined by a system of $m$ linear homogeneous equations where $m$ is the dimension of $I$. Hence $\dim(J) \geq \dim(L) - \dim(I)$. Since $I \cap J = (0)$, this implies $L = I + J$.

Now $L = [L,L] + J$ where $J$ is an ideal and $J \cap [L,L] = (0)$. But then $J \subset$ center of $L$ which is (0). Thus $L = [L,L]$. Q.E.D.

We are now going to define the Casimir operator for a representation of a semi-simple Lie algebra.

Let $L$ be a semi-simple finite dimensional Lie algebra and $\rho$ a finite dimensional representation of $L$. Let $P$ be the kernel of $\rho$. Then $L = P \oplus Q$ (direct sum) with $Q$ an ideal. $Q$ is actually unique for if $Q_1$ is another ideal so that $P \oplus Q_1 = L$, then $[Q_1, Q_1] \subset [Q_1, P \oplus Q] = [Q_1, Q] \subset Q$. Since $L = [L,L]$ and since $Q_1$ is a direct ideal summand in $L$ we have $Q_1 = [Q_1, Q_1]$. Hence $Q_1 \subset Q$. By symmetry, $Q_1 = Q$.

Now $\rho$ induces a faithful representation of $Q$ and $Q$ is semisimple because an ideal of $Q$ is an ideal of $L$. Hence the trace form $f$ of this representation is non-degenerate. With each $u = \sum x_i \otimes y_i$ in $Q \otimes Q$ we associate the linear transformation $u^*$ of $Q$ such that

$$u^*(z) = \sum_i f(z, x_i)\, y_i \quad .$$

(The existence of the map $u \longrightarrow u^*$ is an evident consequence of the mapping property of the tensor product.) The map $u \longrightarrow u^*$ is a monomorphism. In fact, if $y_1, \ldots, y_n$ is a basis of $Q$, then each

$u \in Q \otimes Q$ can be written $\sum_{i=1}^{n} x_i \otimes y_i$ . If $u^* = 0$ then

$\sum_{i=1}^{n} f(z, x_i)y_i = 0$ whence $f(z, x_i) = 0$ for all $z$ in $Q$, $i = 1, \ldots, n$ .

Since $f$ is non-degenerate, $x_i = 0$ whence $u = 0$. Since

$\dim(Q \otimes Q) = \dim(\mathrm{Hom}_K(Q,Q))$, it follows that this map $u \longrightarrow u^*$ is an isomorphism of $Q \otimes Q$ onto $\mathrm{Hom}_K(Q,Q)$. Hence there is one and only one $u_\rho$ in $Q \otimes Q$ such that $u_\rho^*$ is the identity map: $Q \longrightarrow Q$ .

Suppose $U$, $V$ are $L$-modules. We make $U \otimes V$ into an $L$-module such that

$$x.(u \otimes v) = (x.u) \otimes v + u \otimes x.v \quad .$$

In this sense, regard $Q \otimes Q$ as an $L$-module. We claim $L.u_\rho = 0$ . Since $P$ annihilates $Q \otimes Q$, it suffices to show that $Q.u_\rho = 0$ . Write $u_\rho = \sum x_i \otimes y_i$ and take $z$ in $Q$. Then

$$z.u_\rho = \sum [z, x_i] \otimes y_i + \sum x_i \otimes [z, y_i] \quad .$$

Hence for $x \in Q$,

$$(z.u_\rho)^*(x) = \sum_i (f(x, [z, x_i])\, y_i + f(x, x_i)[z, y_i]$$

$$= \sum_i f([x, z], x_i)\, y_i + [z, x]$$

$$= [x, z] + [z, x] = 0 \quad .$$

Thus $(z.u_\rho)^* = 0$ where $z.u_\rho = 0$ .

$u_\rho$ is called the <u>Casimir element of $\rho$ in $L \otimes L$.</u>

Let $C_\rho$ be the canonical image of $u_\rho$ in the universal enveloping algebra $U(L)$ of $L$ under the canonical map: $L \otimes L \longrightarrow U(L)$ ( $\sum x_i \otimes y_i \longrightarrow \sum x_i y_i$). If $U(L)$ is considered as an $L$-module

such that $x.u = xu - ux$ for all $x \in L$, $u \in U(L)$, then the canonical map $L \otimes L \longrightarrow U(L)$ is an L-module homomorphism. Hence $C_\rho$ lies in the center of $U(C)$. Evidently $C_\rho$ also lies in $LU(L)$.

$C_\rho$ is called the Casimir element of $\rho$ in the universal enveloping algebra. We still denote by $\rho$ the canonical extension of $\rho$ to a unitary representation of $U(L)$. Then $\rho(C_\rho)$ is called the Casimir operator of $\rho$

Since $C_\rho$ lies in the center of $U(L)$, $\rho(C_\rho)$ commutes with every L-operator on the representation space of $\rho$. We claim that if $\rho \neq 0$, then $\rho(C_\rho)$ is not nilpotent. Let $y_1, \ldots, y_n$ be a basis for $Q$ and write $u_\rho = \sum_{i=1}^{n} x_i \otimes y_i$. Then

$$\rho(C_\rho) = \sum_{i=1}^{n} \rho(x_i)\rho(y_i) .$$

Thus $T(\rho(C_\rho)) = \sum_{i=1}^{n} T(\rho(x_i)\rho(y_i)) = \sum_{i=1}^{n} f(x_i, y_i)$.

Since $u_\rho^*$ is the identity,

$$\sum_{i=1}^{n} f(y_j, x_i)y_i = u_\rho^*(y_j) = y_j .$$

Thus $f(y_j, x_i) = \delta_{ji}$. Hence $\sum_{i=1}^{n} f(x_i, y_i) = \dim Q$.

Therefore $T(\rho(C_\rho)) = n \neq 0$ so that $\rho(C_\rho)$ cannot be nilpotent.

Theorem 8. Let $L$ be a finite dimensional semi-simple Lie algebra. Then every finite dimensional representation space of $L$ is semi-simple.

Proof: Let $M$ be a finite dimensional L-module and let

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = (0)$$

be a composition series for $M$. Then each L-module, $M_i/M_{i+1}$ is

is either one dimensional and trivial or is simple and non-trivial.

Let $0 \leqq i_o \leqq \ldots \leqq i_m \leqq n-1$ be the indices $i$ for which $M_i/M_{i+1}$ is non-trivial and let $\gamma_q$ be the Casimir operator of the representation of $L$ in $M_{i_q}/M_{i_{q+1}}$. Then each $\gamma_q$ is an $L$-automorphism of $M_{i_q}/M_{i_{q+1}}$. Let $f_q(x) \in K[x]$ be the minimum polynomial of $\gamma_q$ normalized so that the constant term is $1$. Let $c_q$ be the Casimir element (in the universal enveloping algebra) of the representation of $L$ in $M_{i_q}/M_{i_{q+1}}$ and put $d_q = f_q(c_q) - f_q(0) = f_q(c_q) - 1$. Then $d_q$ is a non-zero element of $LU(L)L$, lies in the center of $U(L)$ and $1 + d_q$ annihilates $M_{i_q}/M_{i_{q+1}}$ ($1 + d_q = f_q(c_q) \longrightarrow f_q(\gamma_q) = 0$). Hence, if $x_1, \ldots, x_{n-m+1}$ are arbitrary elements of $L$, $x_1 \ldots x_{n-m+1}(1+d_o) \ldots (1 + d_m)$ annihilates $M$. Since $L = [L, L]$, every element of $L$ can be written (in $U(L)$) as a sum of products of $n-m+1$ elements of $L$. Hence $L(1+d_o) \ldots (1 + d_m)$ annihilates $M$. Thus

$$(1 + d_o)\ldots(1+d_m).M \subset M^L = \{x | x \in M,\ L.x = (0)\}$$

which means that

$$M = L.M + M^L .$$

Let $W \subset V$ be a pair of $L$-modules and let $\pi$ denote the canonical epimorphism: $V \longrightarrow V/W$. Let $M$ be the subset of all $f \in \mathrm{Hom}_K(V/W, V)$ for which $L.f \subset \mathrm{Hom}_K(V/W, W)$. (If $A$ and $B$ are arbitrary $L$-modules we make $\mathrm{Hom}_K(A,B)$ into an $L$-module such that

$$(x.f)(a) = x,f(a) - f(x.a)$$

for all $f \in \mathrm{Hom}_K(A,B)$, $x \in L$ and $a \in A$.)

[illegible] $\mathfrak{M}$-module of $\mathrm{Hom}_K(V/\mathfrak{M}, V)$. By the above, $M = L.M + M^L$. There exists $f \in \mathrm{Hom}_K(V/\mathfrak{M}, V)$ such that $\pi \circ f$ is the identity map: $V/\mathfrak{M} \longrightarrow V/W$. If $x \in L$, $u \in V/W$ then

$$\begin{aligned} \pi(x.f)(u) &= \pi(x, f(u) - f(x.u)) \\ &= x.\pi f(u) - \pi f(x.u) \\ &= x.u - x.u = 0. \end{aligned}$$

Therefore $(x.f)(V/\mathfrak{M}) \subset W$ so that $f$ is in $M$. Write $f = g + h$ with $g \in L.M$, $h \in M^L$. Then $g \in \mathrm{Hom}_K(V/\mathfrak{M}, \mathfrak{M})$ whence $\pi \circ h = \pi \circ f =$ identity on $V/\mathfrak{M}$. Also $L.h = 0$. This means that $h$ is an $L$-homomorphism: $V/W \longrightarrow V$; hence $V = W \oplus h(V/\mathfrak{M})$. Q. E. D.

Theorem 9. Let $L$ be a finite dimensional semi-simple Lie algebra and let $\pi$ be a Lie algebra epimorphism of $E$ onto $L$. Then there exists a Lie algebra monomorphism $\phi : L \longrightarrow E$ such that $\pi \circ \phi$ is the identity on $L$.

Proof: We proceed by induction on the dimension of the kernel, $P$, of $\pi$. If $\dim(P) = 0$ there is nothing to prove so we assume $\dim(P) > 0$ and the theorem true for kernels of lower dimension. If $E$ is semi-simple then, by Theorem 7, $E = P \oplus Q$ where $Q$ is an ideal of $E$ and $\pi$ induces an isomorphism of $Q$ onto $L$. Thus we may suppose that $E$ has a non-zero abelian ideal. Let $A$ be a non-zero abelian ideal of minimal dimension. Then $(A + P)/P$ is an abelian ideal of $E/P \cong L$. Thus, since $L$ is semi-simple, $(A + P)/P = (0)$, so that $A \subset P$.

Suppose first that $A \neq P$. Then we consider the epimorphism $\bar{\pi}$: $E/A \longrightarrow L$ induced by $\pi$. The kernel of $\bar{\pi}$ is $P/A$ whence, by the

induction hypothesis, there exists a monomorphism $\bar{\phi}$: L ---> E/A such that $\bar{\pi} \circ \bar{\phi}$ is the identity on L. Let F be the inverse image in E of $\bar{\phi}(L)$ ($\subset$ E/A) with respect to the canonical epimorphism E ---> E/A. Since dim(A) < dim(P) it follows that the canonical epimorphism $\rho$: F ---> F/A = $\bar{\phi}(L) \cong$ L has an "inverse" $\sigma$: $\bar{\phi}(L)$ ---> F and the composite, $\sigma \circ \bar{\phi}$, satisfies the requirements of Theorem 9.

There remains the case A = P. Then P is abelian and can now be regarded as an L-module via E, i.e., $\pi(e).m = [e,m]$ for all e $\in$ E, m $\in$ P. The L-submodules of P are precisely the ideals of L contained in P. Since dim(P) is minimal, P is a simple L-module.

Suppose first that P is a trivial L-module, i.e., [E, P] = (0). Then E may be regarded as an L-module and $\pi$ is also an L-module epimorphism of E onto L. By Theorem 7 there exists an L-module monomorphism $\phi$: L ---> E such that $\pi \circ \phi$ = identity on L. Since [E, P] $\neq$ (0), $\phi$ is also a Lie algebra monomorphism: L ---> E and we are done.

There remains the case where P is a simple non-trivial L-module. In this case, let $u = \sum x_i \otimes y_i \in L \otimes L$ be the Casimir element of the representation of L in P and let $\gamma$ be the corresponding Casimir operator. $\gamma$ is an automorphism of the L-module P.

Let f be any linear map of L into E such that $\pi f$ = identity on L and define a bilinear map g: L $\times$ L ---> P such that

$$g(x, y) = [f(x), f(y)] - f([x,y]).$$

g is alternating, i.e. g(x,x) = 0, bilinear and, because of the Jacobi identity, g satisfies the identity

$$x.g(y, z) - y.g(x, z) + z.g(x, y) =$$

$$= g([x, y], z) - g([x, z], y) + g([yk z], x).$$

Now consider

$$\gamma(g(x, y)) = \sum_i x_i.(y_i.g(x,y)).$$

$$y_i.g(x,y) = x.g(y_i, y) - y.g(y_i, x)$$

$$+ g([y_i, x], y) - g([y_i, y], x)$$

$$+ g([x,y], y_i) .$$

Hence

$$x_i.y_i.g(x, y) = x_i x.g(y_i, y) - x_i y.g(y_i, x) + x_i.g([y_i, x], y)$$

$$- x_i.g([y_i, y], x) + x_i.g([x, y], y_i)$$

$$= xx_i.g(y_i, y) + [x_i, x].g(y_i, y) - yx_i.g(y_i, x)$$

$$- [x_i, y].g(y_i, x) + x_i.g([y_i, x], y)$$

$$- x_i.g([y_i, y], + x_i.g([x, y], y_i) .$$

Now $\sum_i [x_i, x] \otimes y_i + x_i \otimes [y_i, x]$ is in L.u = (0). It follows, by the universal mapping property of the tensor product, that if h is any bilinear function

$$\sum_i h([x_i, z], y_i) + h(x_i, [y_i, z]) = 0.$$

Applying this remark with $h(u, v) = u.g(v, y)$ for fixed y, we see that

$$\sum_i [x_i, x].g(y_i, y) + x_i.y([y_i, x], y) = 0.$$

Similarly,

$$\sum_i [x_i, y].g(y_i, x) + x_i.g([y_i, y], x) = 0.$$

Hence, summing over i, the above reduces to

$$\gamma(g(x, y)) = \sum_i (xx_i.g(y_i, y) - yx_i.g(y_i,x) + x_i.g([x, y], y_i)).$$

Now put $h(x) = \sum_i x_i.g(y_i, x)$ . Then our result reads

$$\gamma(g(x, y)) = x.h(y) - y.h(x) - h([x, y])$$

or

$$g(x, y) = x.\gamma^{-1}h(y) - y.\gamma^{-1}h(x) - \gamma^{-1}h([x, y]).$$

From this it is easily verified that the map $\phi = f - \gamma^{-1}h$ satisfies the requirements of the theorem.

Suppose L is a Lie algebra and A is an ideal of L. Then if L is solvable, so is L/A. If A is solvable and L/A is solvable then L is solvable. Define $L_1 = L, \ldots, L_{i+1} = [L_i, L_i]$. Clearly $(L/A)_n = (L_n = A)/A$; hence if L is solvable so is L/A. If L/A is solvable, the above shows that $L_n \subset A$ for large enough n; hence if A is solvable, so is L.

Now the isomorphism $(A + B)/A \cong A/A \cap B$ shows that if A and B are solvable ideals of L, so is A + B. Hence, assuming L is finite dimensional, the sum, R, of all solvable ideals of L is a solvable ideal containing every solvable ideal of L. <u>R is called the radical of L.</u> It follows easily that L/R is semi-simple. Let A be an ideal of L, then (A + R)/R is an ideal of the semi-simple Lie algebra L/R. Hence (A + R)/R is semi-simple. But $(A + R)/A \cong A/A \cap R$ and it follows that $A \cap R$ must contain the radical of A. On the other hand,

$A \cap R$ is a solvable ideal of $A$ and thus must be contained in the radical of $A$. Hence, the radical of an ideal $A$ of $L$ is the intersection with $A$ of the radical of $L$.

Consider the epimorphism $L \dashrightarrow L/R$. By Theorem 8 this can be inverted so that $L = S + R$ where $S$ is a semi-simple subalgebra of $L$ and $S \cap R = (0)$. This is called a Levi-decomposition of $L$.

Now $[L, L] = S + [L, R]$ so that $[L, R]$ is the radical of $[L, L]$ and coincides with $[L, L] \cap R$. If $M$ is a finite dimensional $L$-module then $[L, R]$ is nilpotent on $M$. To see this, note first that $[R, R]$ is nilpotent on $M$ by Theorem 4. Now let $S$ be a subspace of $[L, R]$ containing $[R, R]$ and nilpotent on $M$. If $S \neq [L,R]$, there exists $z \in L$, $x \in R$ such that $[z, x] \in S$. Since $[z, x]$ is nilpotent on $M$ it follows from Lemma 4 that $K[z, x] + S$ is nilpotent on $M$. Hence, we see inductively that $[L, R]$ is nilpotent on $M$. Thus we have

Theorem 10. Let $L$ be a finite dimensional Lie algebra and let $R$ be the radical of $L$. Let $M$ be any finite dimensional $L$-module. Then $[L, R] \cap R$ is nilpotent on $M$.

In particular, $[L, R]$ is nilpotent on $L$. Hence, for every $x \in [L, R]$, we can form the polynomial

$$\exp D_x = \sum_{i=0}^{n} \frac{1}{i!} D_x^i$$

where $n$ is the smallest integer such that $D_x^{n+1} = 0$. Clearly, $\exp D_x$ is a Lie algebra automorphism of $L$ ( its inverse is $\exp(-D_x)$). Denote by $G_L$ the group of Lie algebra automorphisms generated by the $\exp D_x$ as $x$ runs through $[L, R]$.

Theorem 11. (Malcev, Harish-Chandra). Let $L$ be a finite dimensional Lie algebra and let $R$ be the radical of $L$. Let $L = S + R$ be a Levi-decomposition and $T$ any semi-simple subalgebra of $L$. Then there exists $\alpha$ in $G_L$ such that $\alpha(T) \subset S$.

Proof: For every $t \in T$ write $t = \sigma(t) + \rho(t)$ with $\sigma(t)$ in $S$, $\rho(t)$ in $R$.

$$[\sigma(t_1) + \rho(t_1), \sigma(t_2) + \rho(t_2)] = \sigma([t_1, t_2]) + \rho([t_1, t_2]) .$$

Hence

$$[\sigma(t_1), \sigma(t_2)] = \sigma([t_1, t_2])$$

and

$$[\sigma(t_1), \rho(t_2)] - [\sigma(t_2), \rho(t_1)] + [\rho(t_1), \rho(t_2)] = \rho([t_1, t_2]).$$

Since $T = [T, T]$, it follows that $\rho(T) \subset [L, R]$. Let $f(t)$ be the coset of $\rho(t)$ mod $[R,R]$. Then $f$ is a linear map of $T$ into $[L, R]/[R, R]$. If we equip $[L, R]/[R, R]$ with its natural structure as a $T$-module, the above relation shows that

$$f([t_1, t_2]) - t_1 . f(t_2) - t_2 . f(t_1) = 0 .$$

Hence, $f$ can be used to define a $T$-module structure on the space $(K, [L, R]/[R, R])$ such that

$$t . (\alpha, u) = (0, \alpha f(t) + t . u)$$

for $t \in T$, $\alpha \in K$ and $u \in [L, R]/[R, R]$.

Since $T$ is semi-simple, this $T$-module is semi-simple. Hence, the submodule $(0, [L, R]/[R, R])$ has a module complement. Choosing $u$ in $[L, R]/[R, R]$ so that $(1, u)$ is in this module complement, we see that

$$t . (1, 0) = t . (1, u) - t . (0, u) .$$

It follows that

$$f(t) = t.u \quad .$$

Let $x$ be an element of $[L, R]$ whose coset mod $[R, R]$ is $u$. Then $\rho(t) - [t, x]$ is in $[R, R]$ whence $t - [t, x]$ is in $\sigma(t) + [R, R]$. Therefore

$$\exp(D_x)(t) = t + [x, t] + \frac{1}{2} D_x^2(t) + \ldots$$

$$\in \sigma(t) + \frac{1}{2} D_x^2(t) + \ldots + [R, R]$$

$$\subset \sigma(t) + [R, R] .$$

Thus $\exp(D_x)(T) \subset S + [R,R]$. Proceeding by induction on $\dim(R)$ we see that the induction hypothesis gives $\beta \in G_{S+[R,R]}$ such that $\beta(\exp(D_x)(T)) \subset S$. This shows that there is an element $\alpha$ of $G_L$ such that $\alpha(T) \subset S$. Q.E.D.

## 4. Extensions of Representations.

Let $\rho$ be a representation of $L$ with representation space $V$. Let $V = V_0 \supset V_1 \supset \ldots \supset V_n = (0)$ be a composition series for $V$. Define $V' = \sum \oplus V_j/V_{i+1}$. By the Jordan-Holder theorem, $V'$ is determined by $V$ up to an $L$-isomorphism. Let $\rho'$ be the induced representation of $L$ in $V'$. Then $\rho'$ is called the semi-simple representation associated with $\rho$. If $S$ is a subalgebra of $L$ and if $\rho(S)$ is nilpotent on $V$ we shall say that $\rho$ is nilpotent on $S$.

Lemma 5. Let $L$ be a finite dimensional Lie algebra and $P$ an ideal of $L$. Suppose $L = H + P$ where $H$ is a subalgebra of $L$ and $H \cap P = (0)$. Let $\rho$ be a finite dimensional representation of $P$ and suppose that $\rho'[H, P] = (0)$. Then the representation space, $V$, of $\rho$ can be

P-monomorphically imbedded in a finite dimensional representation space W of L. If $\sigma$ is the representation of L on W then the kernel of $\sigma'$ contains the kernel of $\rho'$. If H is nilpotent on P then the kernel of $\sigma'$ also contains H.

Proof: Let U(L), U(P) be the universal enveloping algebras of L and P respectively. Identify U(P) with its canonical image in U(L). If $u \in U(P)$, $h \in H$, $p \in P$, define

$$u.(h + p) = (uh - hu) + up \in U(P).$$

It is verified immediately that for $x, y \in L$, $u \in U(P)$,

$$(u.x).y - (u.y).x = u.[x, y] .$$

Thus U(P) becomes a right L-module and hence a unitary right U(L)-module.

Let I and I' denote the kernels in U(P) of $\rho$ and $\rho'$ respectively. These are ideals of finite codimension in U(P). Let $d = [V:K]$; then $(I')^d \subset I$. By Theorem 2, $(I')^d$ is also of finite codimension in U(P). By hypothesis, $[H, P] \subset I'$ whence $(I')^d$ is a U(L)-submodule of U(P). In fact, $U(P).H \subset I'$. Therefore we can consider $U(P)/(I')^d$ as a right unitary U(L)-module. This gives the structure of a unitary left U(L)-module on $\mathrm{Hom}_K(U(P)/(I')^d, V)$ where, for $x \in U(L)$, $f \in \mathrm{Hom}_K(U(P)/(I')^d, V)$, $\bar{u} \in U(P)/(I')^d$,

$$(x.f)(\bar{u}) = f(\bar{u}.x) .$$

Every element of $v \in V$ defines an element $f_v$ of $\mathrm{Hom}_K(U(P)/(I')^d, V)$ as follows:

$$f_v(\bar{u}) = \bar{u}.v$$

for $\bar{u} \in U(P)/(I')^d$. Since U(P) has an identity, the map $v \longrightarrow f_v$

is a $U(P)$-monomorphism of $V$ into $\mathrm{Hom}_K(U(P)/(I')^d, V)$.

Let $\sigma$ be the representation of $L$ (and $U(L)$) on $\mathrm{Hom}_K(U(P)/(I')^d, V)$. Then $\sigma$ is nilpotent on the ideal $I' \cap P$ of $L$ and this implies that $I' \cap P$ lies in the kernel of $\sigma'$. Thus the kernel of $\sigma'$ contains the kernel of $\mathcal{O}'$.

Now assume that $H$ is nilpotent on $P$. Then for every $u$ in $U(P)$ there exists an $n > 0$ such that $u.(h_1 \ldots h_n) = 0$ for all $h_1, \ldots, h_n$ in $H$. Since $U(P)/(I')^d$ is finite dimensional, this shows that $H$ is nilpotent on $U(P)/(I')^d$ and therefore, that $H$ is nilpotent on $\mathrm{Hom}_K(U(P)/(I')^d, V)$. Now $\sigma$ is nilpotent on $H$ and on $I' \cap P$. Then (by the same proof as that of Lemma 4) $\sigma$ is nilpotent on $H + I' \cap P$. This is an ideal of $L$ (because $[H, L] = [H, H + P] \subset H + [H, P] \subset H + I' \cap P$) and therefore $H + I' \cap P$ is contained in the kernel of $\sigma'$. Q.E.D.

Def. Put $L^1 = L, \ldots, L^{i+1} = [L, L^i]$. We say that L is nilpotent if there exists an $n$ such that $L^n = 0$.

The sum of all nilpotent ideals of $L$ is a nilpotent ideal called the maximum nilpotent ideal of $L$. In fact, we have the following general theorem:

Theorem 12. Let $L$ be a finite-dimensional Lie algebra and let $M$ be a finite-dimensional $L$-module. Then the sum of all ideals of $L$ that [illegible] on $M$ is an ideal, $P$, of $L$ that is nilpotent on $M$. [illegible] of the radical of $L$ that is nilpotent on $M$ belongs to $P$.

Proof: It is easy to see that $P$ is simply the kernel of the semi-simple representation of $L$ associated with the representation of $L$ on $M$. There remains only to prove the last assertion.

Let $R$ be the radical of $L$. Then, by Theorem 9, $[R, L] \subset P \cap R \subset R$.

Now let $x$ be in $R$ and suppose $x$ is nilpotent on $M$. Then, by Lemma 4, $(x) + P \cap R$ is nilpotent on $M$. Since this is an ideal of $L$, it follows that $x$ is in $P$.

Theorem 13. (Ado). Let $L$ be a finite dimensional Lie algebra. Then there exists a faithful finite dimensional representation of $L$ that is nilpotent on the maximum nilpotent ideal of $L$.

Proof: Let $Z$ be the center of $L$, $N$ the maximum nilpotent ideal and $R$ the radical. Then $Z + [L, R] \subset N \subset R$. Let $N = N_0 \supset \ldots \supset N_r = Z$ be a series of ideals of $N$ such that $N_i/N_{i+1}$ is one dimensional. Then, for each $i$, $N_i = Kn_i + N_{i+1}$ (semi-direct sum) with $n_i \in N_i$. Start with a faithful representation of $Z$. Apply Lemma 5 repeatedly to the semi-direct sums $Kn_i + N_{i+1}$ to obtain a nilpotent representation of $N$ that is faithful on $Z$.

Let $R = R_0 \supset \ldots \supset R_q = N$ be a chain of ideals of $L$ (every subspace of $R$ containing $N$ is an ideal) such that $R_i/R_{i+1}$ is one dimensional and write $R_i = Kr_i + R_{i+1}$. Again by Lemma 5, our representation of $N$ can be extended to a representation of $R$ that is still nilpotent on $N$.

Finally let $L = S + R$ be a Levi-decomposition of $L$. Since $[L, R] \subset N$ we can (by Lemma 5) extend our representation of $R$ to a representation of $L$ which is still nilpotent on $N$. Thus we have a representation of $L$, faithful on $Z$ and nilpotent on $N$. The direct sum of this representation and the adjoint representation satisfies the requirements of our theorem.

Theorem 14. Let L be a finite dimensional Lie algebra and let T be a term of a normal series for L. Let J be the radical of T. Let $\rho$ be a finite dimensional representation of T, with representation space M, such that $\rho$ is nilpotent on $[L, L] \cap J$. Then M can be T-monomorphically imbedded in a representation space N for a representation $\sigma$ of L and the kernel of $\sigma'$ contains the kernel of $\rho'$.

Proof: We proceed by induction on the dimension of the factor space L/T. Suppose the theorem true for the lower cases and $L \neq T$. Then there exists a term $T_1$ of a normal series for L such that T is an ideal of $T_1$ and $T_1/T$ is a simple Lie algebra. Let $J_1$ and J be the radicals of $T_1$ and T respectively. We now distinguish two cases.

1° $T_1/T$ is non-abelian and therefore semi-simple. Then $J = J_1$ since $J = J_1 \cap T$ so that $(J_1 + T)/T \cong J_1/J$ is a solvable ideal of $T_1/T$. Now choose a Levi-decomposition $T_1 = S_1 + J$. T is an ideal of $T_1$ so that $S_1 \cap T$ is an ideal of $S_1$. Hence, by Theorem 7, we may choose an ideal $U_1$ of $S_1$, so that $S_1 = U_1 \oplus (S_1 \cap T)$. Thus $T_1 = U_1 + T$ (semi-direct sum), $T = S_1 \cap T + J$, whence $[U_1, T] \subset J$. Now $\rho$ is nilpotent on the ideal $[L, L] \cap J$ so that $[L, L] \cap J$ is in the kernel of $\rho'$ and $\rho'([U_1, T]) = (0)$. Thus we may apply Lemma 5 to extend $\rho$ to a representation $\rho_1$ of $T_1$ such that the kernel of $\rho_1'$ contains the kernel of $\rho'$ and hence $\rho_1$ is nilpotent on $[L, L] \cap J = [L, L] \cap J_1$.

2° $T_1/T$ is one dimensional. Then let $T = S + J$ be a Levi-decomposition of T. By Theorem 11, there exists a semi-simple subalgebra, $S_1$, of $T_1$ such that $T_1 = S_1 + J_1$ and $S_1 \supset S$. Now $S \subset S_1 \cap T$ which is a semi-simple ideal of $S_1$. Since S is a maximal semi-simple

subalgebra of $T$ it follows that $S_1 \cap T = S$. The canonical image of $S_1$ in $T_1/T$ is isomorphic with $S_1/S_1 \cap T \cong S_1/S$ which is semi-simple. Hence, $S_1 = S$. Thus $T_1 = S + J_1$ and $J_1/J$ is one-dimensional. Now suppose $[L, L] \cap J_1 = [L, L] \cap J$. Then we can apply Lemma 5 to extend $\rho$ to a representation $\rho_1$ of $T_1$ which is still nilpotent on $[L, L] \cap J_1$.

If $[L, L] \cap J_1 \neq [L, L] \cap J$, choose $x$ in $[L, L] \cap J_1$ such that $x \notin [L, L] \cap J$. Then $T_1 = (x) + T$. Applying Lemma 5 to this semi-direct sum, noting that $x$ is nilpotent on $T$, we see that $\rho$ can be extended to a representation $\rho_1$ of $T_1$ such that

$$\rho_1((x) + [L, L] \cap J) = (0).$$

Since

$$(x) + [L, L] \cap J = [L, L] \cap J_1,$$

$\rho_1$ is nilpotent on $[L, L] \cap J_1$.

This completes the inductive step.

## Part II

## [illegible] GROUPS AND THEIR LIE ALGEBRAS

### 1. The algebraic hull of a linear Lie Algebra

Let $V$ be a finite dimensional vector space over an infinite field $F$ and let $A = \mathrm{Hom}_F(V, V)$. Let $P$ denote the algebra of all polynomial functions on $A$; $P$ is the algebra generated by the constant functions and by $E^* = \mathrm{Hom}_F(E, F)$. Since the ground field is infinite we may identify $P$ with the symmetric algebra over $E^*$.

**Def.** A group $G$ of automorphisms of $V$ is called an algebraic linear group if it is the set of all automorphisms of $V$ that are zeros of a subset of $P$.

We may regard $P$ as a two-sided $E$ module with $E$ acting on $P$ by right and left translation, i.e. for $e \in E$, $p \in P$, $x \in E$,

$$(p.e)(x) = p(ex) \quad , \quad (e.p)(x) = p(xe) \ .$$

For $e \in E$, $D_e$ denotes the derivation of $P$ which annihilates $F$ and coincides with left translation by $e$ on $E^*$.

Let $Q$ be the set of all elements of $P$ whose restrictions to the algebraic group $G$ are 0. $Q$ is clearly an ideal of $P$, called the ideal of polynomial functions associated with $G$. The set of all $e$ in $E$ such that $D_e(Q) \subset Q$ is a Lie subalgebra of $E$, called the Lie algebra of $G$ and is denoted by $G^\circ$ .

Prop. 1. Let $A$ and $B$ be algebraic groups of automorphisms of $E$ such that $A \subset B$. Then $A^\circ \subset B^\circ$ .

Proof: Let $\mathcal{A}$ and $\mathcal{B}$ be the ideals associated with $A$ and $B$ respectively. Suppose $e$ is in $A^\circ$ . Then, since $\mathcal{B} \subset \mathcal{A}$, $D_e(\mathcal{B}) \subset \mathcal{A}$. Let $p$ be in $\mathcal{B}$, $b \in B$ and $I$ the identity transformation on $V$. Then $p.b$

is in $\mathfrak{L}$ whence $D_e(p.b)$ is in $\mathfrak{M}$ and so $D_e(p.b)\{I\} = 0$. Now since left translations commute with right translations, it follows that $D_e$ commutes with every right translation of P. Hence

$$(D_e(p))\{b\} = (D_e(p).b)\{I\} = D_e(p.b)\{I\} = 0$$

so that $D_e(p) \in \mathfrak{L}$. Thus $D_e(\mathfrak{L}) \subset \mathfrak{L}$ for every e in $A^*$. Therefore $A^* \subset B^*$.

Def. A Lie subalgebra of E is called an algebraic Lie algebra if it is the Lie algebra of an algebraic (linear) group.

Theorem 1. Let V be a finite dimensional vector space over a field F of characteristic 0. Let L be a Lie subalgebra of $E = \mathrm{Hom}_F(V, V)$. Let $G_L$ be the intersection of all algebraic groups of automorphisms of V whose Lie algebras contain L. Then $(G_L)^\circ \supset L$. $(G_L)^\circ$ is called the algebraic hull of L.

Proof: Note that by Proposition 1, $(G_L)^\circ$ is contained in every algebraic Lie algebra containing L.

Take x in E and let $G_x$ be the intersection of all algebraic groups whose Lie algebras contain x. Then $G_x \subset G_L$ whenever x is in L. By Proposition 1 it suffices to prove that x is in $(G_x)^\circ$. Thus it suffices to prove the theorem when L is one-dimensional.

Let t be an indeterminate over F and let $F\{t\}$ be the ring of integral power series with coefficients in F. We extend the elements of $E^*$ uniquely to $F\{t\}$ linear maps of $E \otimes_F F\{t\}$ into $F\{t\}$. The elements of P are extended accordingly to $F\{t\}$ - valued functions on $E \otimes_F F\{t\}$.

With x in E, we interpret the formal power series $\exp(tx)$ as

the element of $E \otimes_F F\{t\}$ that is determined by the condition:

$$p(\exp(tx)) = \sum_{n=0}^{\infty} \frac{p(x^n)t^n}{n!}$$

for every $p$ in $E^*$ .

Now we consider the F-algebra homomorphism $p \longrightarrow p(\exp(tx))$ of $P$ into $F\{t\}$ . Let $\delta$ be the derivation with respect to $t$ in $F\{t\}$ , then

$$(*) \qquad D_x(p)(\exp(tx)) = \delta(p(\exp(tx)) \quad .$$

To see this, note that if $p$ is in $F + E^*$, say $p = a + e^*$ , then $D_x(p) = x.e^*$ . Thus

$$D_x(p)(\exp(tx)) = \sum_{0}^{\infty} \frac{e^*(x^{n+1})}{n!} t^n = \delta(p(\exp(tx))) \quad .$$

Now the maps $p \longrightarrow D_x(p)(\exp(tx))$ and $p \longrightarrow \delta(p(\exp(tx)))$ are both differentiations of $P$ into $F\{t\}$ which coincide on a set of generators and hence are equal. This verifies (*).

Let $Q$ be the kernel of the homomorphism $p \longrightarrow p \exp(tx)$ and let $G$ be the set of all automorphisms of $V$ that are zeros of $Q$. We show first that $G$ coincides with the group $H$ of all automorphisms $h$ of $V$ such that $Q.h = Q$.

Note that for every $p \in P$, $p(I)$ is the constant term of $p(\exp(tx))$. Now let $h$ be in $H$ and $q$ in $Q$, then $q.h$ is in $Q$. Hence $(q.h)(\exp(tx)) = 0$ so that $(q.h)(I) = 0$. Thus $q\{h\} = 0$ and therefore $H \subset G$ . Now let $g$ be in $G$, $q$ in $Q$. From (*) we see by

induction that $D_x^n(p)(\exp(tx)) = \delta^n(p(\exp(tx))$ for every $n \geq 0$ and therefore $D_x^n(q)$ is in $Q$ for every $n \geq 0$. Hence $D_x^n(q.g)\{I\} = (D_x^n(q).g)\{I\} = D_x^n(q)\{g\} = 0$. Again using (*) we find that $q.g$ is in $Q$, i.e. that all the coefficients of $(q.g)(\exp(tx))$ are 0. Therefore $Q.g \subset Q$. Let $Q_d$ be the subspace of $Q$ consisting of all elements of degree $\leq d$. Then $Q_d$ is finite dimensional and $Q_d.g \subset Q_d$. Now $g$ is an automorphism of $V$ and thus has an inverse in $E$. This means that translation by $g$ is an automorphism of $P$ and hence induces a monomorphism: $Q_d \dashrightarrow Q_d$ which must therefore also be an epimorphism because of the finite dimensionality of $Q_d$. Therefore $Q_d.g = Q_d$ whence $Q.g = Q$ so that $g$ is in $H$. Thus $G \subset H$ which gives $G = H$.

[If the base field $F$ were algebraically closed, it would follow that the ideal associated with $G$ coincides with $Q$. In fact, let $d$ be the determinant function on $E$ and let $p$ in $P$ be such that $p(G) = 0$, then $pd$ vanishes at every $0$ of $Q$ in $E$. Since $Q$ is a prime ideal and $F$ is algebraically closed, the Hilbert Nullstellensatz gives $pd$ in $Q$. Since $d$ is not in $Q$, $p$ is in $Q$. Thus $Q$ is the ideal associated with $G$ so that $x$ belongs to $(G_x)'$. ]

Let $T$ be an algebraic group of automorphisms of $V$ such that $x$ is in $T'$. Let $A$ be the ideal of polynomial functions associated with $T$. Then $D_x(A) \subset A$. Hence, for all $p$ in $A$ and all $n \geq 0$, $D_x^n(p)\{I\} = 0$. By (*), $p(\exp(tx)) = 0$, i.e., $p$ is in $Q$. Thus $A \subset Q$. Hence $G \subset T$. Thus $G \subset G_x$.

Next we shall prove that

$$(**) \qquad P/Q \subset F(z_1, \ldots, z_n)$$

where the set $(z_1, \ldots, z_n)$ is algebraically free over $F$.

Suppose (**) is true, and let $Q_1$ be the ideal of polynomial functions associated with G. $Q \subset Q_1$. Suppose $Q \neq Q_1$ and choose b in $Q_1$ such that $b \notin Q$. Let d be the determinant function on E. For $p \in P$, let $p'$ denote its canonical image in /Q. Write

$$b'd' = f(z_1, \ldots, z_n)/g(z_1, \ldots, z_n)$$

where f and g are polynomials. Let $p_1, \ldots, p_n$ be a basis for $E^*$ and write $p_i' = f_i(z_1, \ldots, z_n)/g_i(z_1, \ldots, z_n)$ with $f_i$ and $g_i$ polynomials. There exist elements $s_1, \ldots, s_n$ in F such that $fgg_1 \cdots g_n$ does not vanish at the point $(s_1, \ldots, s_n)$ of $F^n$. Let e be the element of E for which

$$p_i(e) = \frac{f_i(s_1, \ldots, s_n)}{g_i(s_1, \ldots, s_n)} .$$

Then

$$b(e)d(e) = \frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} \neq 0 .$$

This means that e is an automorphism of V and not a zero of b. On the other hand, e is a zero of Q so that e is in G. This is a contradiction. Hence $Q = Q_1$, i.e., Q is the ideal associated with G. Since $D_x(Q) \subset Q$, x is in $G^*$. Thus we need only to verify (**).

If K is any field containing F and A is any vector space or algebra over F, we write $A^K = A \otimes_F K$ and also identify A with its canonical image in $A^K$. We identify $E^K$ with $\mathrm{Hom}_K(V^K, V^K)$. Finally, we identify the algebra of polynomial functions on $E^K$ with $P^K$. Let K be a finite Galois extension of F containing all the characteristic roots of x. The Galois group, S, of K over F operates in the natural fashion on $K\{T\} = K \otimes_F F\{t\}$ and on $P^K$.

The homomorphism $p \longrightarrow p(\exp(tx))$ of $P^K$ into $K\{t\}$ is an S-homomorphism and induces an isomorphism of the F-algebra $P/Q$ onto the F-algebra of the S-fixed elements in the image of $P^K$ in $K\{t\}$ .

We can decompose $V^K$ into the direct sum of x-stable subspaces $V_i$ such that each $V_i$ is annihilated by some power of $x - c_i I$ with $c_i$ in K. Let $x_i$ be the endomorphism of $V_i$ induced by x. Then the image of $P^K$ by the homomorphism $p \longrightarrow p(\exp(tx))$ is generated as a K-algebra by the constants and the power series $p_i(\exp(tx_i))$, where, for each i, $p_i$ ranges over the linear functions $\mathrm{Hom}_K(V_i, V_i)$ . Write $x_i = c_i I + u_i$ with $u_i^{d_i} = 0$. Then

$$p_i(\exp(tx_i)) = \exp(tc_i) \sum_{i=0}^{d_i-1} \frac{p_i(u_i^k)}{k!} t_k \quad .$$

Hence we see that the image of $P^K$ in $K\{t\}$ is contained in the ring $K[t, \exp(tc_1), \ldots, \exp(tc_n)]$ where $c_1, \ldots, c_n$ are all the characteristic roots of x.

Let $a_1, \ldots, a_q$ be a free basis for the additive group generated by $c_1, \ldots, c_p$. We claim that the set $(t, \exp(ta_1), \ldots, \exp(ta_q))$ is algebraically free over K. For suppose that

$$p(x_o, \ldots, x_q) = \sum p_{e_o,\ldots,e_q} x_o^{e_x} \cdots x_q^{e_q}$$

is a polynomial with coefficients in K such that

$$p(t, \exp(ta_1), \ldots, \exp(ta_q)) = 0.$$

Then

$$\sum p_{e_o,\ldots,e_q} t^{e_o} \exp(t(e_1 a_1 + \ldots + e_q a_q)) = 0 .$$

We have

$$\sum e_i a_i = \sum e'_i a_i$$

only if $e_i = e_i'$, for each $i$. Hence, in order to show that $p = 0$, it suffices to prove that if $b_1, \ldots, b_n$ are different elements of $K$, then the set $(\exp(tb_1), \ldots, \exp(tb_n))$ is linearly independent over $K[t]$. This is evident for $n = 1$. Assume $n > 1$ and the result proved for $n - 1$ elements. If $p_i(t) \in K[t]$ are such that

$$\sum_{i=1}^{n} p_i(t) \exp(tb_i) = 0$$

then

$$p_n(t) + \sum_{i=1}^{n-1} q_{i,h}(t) \exp(t(b_i - b_n)) = 0$$

where the $q_{i,h}(t)$ are given by: $q_{i,o}(t) = p_i(t)$ ; $q_{i,h+1}(t) = q_{i,h}^{(1)}(t) + (b_i - b_n)q_{i,h}(t)$ . For some $h$, $p_n^{(h)}(t) = 0$ and the induction hypothesis gives that $q_{i,h}(t) = 0$ . But then the above recursion gives

$$q_{i,h-1} = q_{i,h-2} = \ldots = p_i(t) = 0 .$$

The elements of $S$ permute the $c_i$ among themselves hence the elements of $S$ (acting on the quotient field of $K\{t\}$) permute among themselves the elements of the multiplicative group generated by $t$, $\exp(a_1 t)$ , ..., $\exp(a_q t)$. In particular, $K(t, \exp(a_1 t), \ldots, \exp(a_q t))$ is S-stable. $P/Q$ is isomorphic as an F-algebra with an F-subalgebra of the field of the S-fixed elements of $K(t, \exp(a_1 t), \ldots, \exp(a_q t))$. Hence it suffices to show that the field of S-fixed elements of $K(t, \exp(a_1 t), \ldots, \exp(a_q t))$ is contained in a purely transcendental extension of F.

Lemma 1. Let $K$ be a field and let $L = K(u)$ where $u = (u_1, \ldots, u_r)$ is algebraically free over $K$. Let $M$ be the multiplicative group generated be $u_1, \ldots, u_r$ . Let $S$ be a finite group of automorphisms of $L$ and assume that both $K$ and $M$ are S-stable. Assume also that the restriction

of S to K is a monomorphism of S into the automorphism group of K. Let F be the field of S-fixed elements of K. Then the field of the S-fixed elements of L is contained in a finite, purely transcendental extension of K.

**Proof:** Let $v = (v_{ij})$, $i = i, \ldots, r$, $j = 1, \ldots, n$ where $n = [k : F]$, be a set of indeterminates over K. Also take a basis $k_1, \ldots, k_n$ for K over F. Let $\phi$ be the homomorphism of M into the multiplicative group of K(v) such that

$$\phi(u_i) = \sum_{j=1}^{n} v_{ij} k_j \quad .$$

Let S operate on K(v) coefficient wise. Define the homomorphism $\Psi$ on M by

$$\Psi = \prod_{s \in S} s \circ \phi \, s^{-1} \quad ,$$

then $\Psi \circ S = s \circ \Psi$ for all s in S.

$$s(\phi(u_i)) = \sum_{j=1}^{n} v_{ij} \, s(k_j) \quad .$$

Now the K-linear combinations of the elements of S (regarded as endomorphisms of K) make up the space of all F-linear endomorphisms of K. Hence we see that the $v_{ij}$ can be expressed as K-linear combinations of the $S(\phi(u_i))$ with s in S and $i = 1, \ldots, r$. Hence the $S(\phi(u_i))$ are algebraically free over K.

Let $N_S$ denote the group generated by the elements $s(\phi(u_i))$, $i = 1, \ldots, r$ with s fixed in S, and let N denote the group generated by all elements of the form $s(\phi(u_i))$ with s in S and $i = 1, \ldots, r$. Since the $s(\phi(u_i))$ are algebraically free, N is the direct product of the $N_S$. Now $\phi$ is an isomorphism of M onto N, hence $s \circ \phi \circ s^{-1}$ is an isomorphism of M onto $N_S$ and therefore, $\Psi$ is a monomorphism

of M into N. Since the elements of N are K-linearly independent, $\psi$ extends uniquely to a K-algebra monomorphism from K(M) to K(N). The field of S-fixed elements of K(M) is mapped into the field of S-fixed elements of K(N), i.e., the field of the S-mixed elements of K(u) is mapped into the field of the S-fixed elements of K(v), i.e., into F(v). This completes the proof of Theorem 1.

## 2. Representative Functions.

Let L be a finite-dimensional Lie algebra over a field F of characteristic 0 and let U denote the universal enveloping algebra of L. We consider finite-dimensional representations of L or U. We let $E = \mathrm{Hom}_F(V, V)$, where V is a unitary U-module, and $E^* = \mathrm{Hom}_F(E, F)$.

If $\tau$ is in $E^*$ and $\rho$ is the given representation mapping U into E, then $\tau \circ \rho$ is called a representative function on U associated with $\rho$. These functions make up a finite dimensional subspace, $R(\rho)$, of $U^* = \mathrm{Hom}_F(U, F)$. The kernel I of $\rho$ in U is an ideal of finite codimension in U and the elements of $R(\rho)$ all vanish on I. Conversely, if f is in $U^*$ and if f vanishes on an ideal I of finite codimension then f is a representative function. In fact, $U^*$ is a left unitary U-module under $(x.f)(u) = f(ux)$ for all x, u in U, $f \in U^*$. If f vanishes on I then f generates a finite dimensional U-submodule of $U^*$. Let $\rho$ be the representation of U on this submodule, then f is associated with $\rho$: $f = \tau \circ \rho$ where $\tau(e) = e(f)$ $\{1\}$. In fact, $\tau \circ \rho(x) = \tau(\rho(x)) = \rho(x)(f)$ $\{1\} = (x.f)(1) = f(x)$ for all x in U.

Let d denote the F-homomorphism: $L \longrightarrow U \otimes U$ such that $d(x) = x \otimes 1 = 1 \otimes x$ for all x in L. We may extend d to an F-algebra

homomorphism $d_T$ of the tensor algebra over L and

$$\begin{aligned} d_T(x \otimes y - y \otimes x - [x, y]) &= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) \\ &\quad - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x) \\ &\quad - [x, y] \otimes 1 - 1 \otimes [x, y] \\ &= xy \otimes 1 + 1 \otimes xy - yx \otimes 1 \\ &\quad - 1 \otimes yx - [x, y] \otimes 1 - 1 \otimes [x, y] \\ &= 0 . \end{aligned}$$

Thus d induces an F-algebra homomorphism of U into $U \otimes U$ which we still denote by d.

We shall define a multiplication in $U^*$ in the following way: for $f, g \in U^*$ then $f \otimes g$ is the element of $(U \otimes U)^*$ such that $(f \otimes g)(u_1 \otimes u_2) = f(u_1)g(u_2)$ . Now define $\underline{(fg)(u) = (f \otimes g)(du)}$, i.e., the multiplication $U^* \otimes_F U^* \longrightarrow U^*$ is the dual of d. This multiplication is associative because $(d \otimes 1) \circ d = (1 \otimes d) \circ d$ and it is obviously commutative.

Suppose f and g are elements of $U^*$ such that f vanishes on an ideal I of U and g vanishes on an ideal J of U. Then fg vanishes on $d^{-1}(I \otimes_F U + U \otimes_F J)$ . d induces a monomorphism of $U/d^{-1}(I \otimes U + U \otimes J)$ into $U \otimes U/(I \otimes U + U \otimes J) \cong U/I \otimes U/J$. Hence, if I and J are of finite codimension in U, then fg vanishes on an ideal of finite codimension in U. Let R denote the algebra of all representative functions. Then R is a subalgebra of $U^*$ .

Suppose $\rho$ and $\sigma$ are two representations of U within the endomorphism algebras A and B. If X and Y are the representation spaces associated with $\rho$ and $\sigma$ respectively, then $\rho \otimes \sigma$ may be regarded as

a representation of $U$ with representation space $X \otimes Y$ such that for $z$ in $L$, $x$ in $X$ and $y$ in $Y$,

$$(\rho \otimes \sigma)(z)(x \otimes y) = \rho(z)(x) \otimes y + x \otimes \sigma(z)(y).$$

$X \otimes Y$ may be regarded as a $U \otimes U$-module. Then the $U$-module structure on $X \otimes Y$ is given by

$$u * w = d(u).w$$

for all $u$ in $U$, $w$ in $X \otimes Y$. Furtner, if $s$ and $t$ are elements of $A^*$ and $B^*$ respectively, it is easily verified that

$$(s \circ \rho)(t \circ \tau) = (s \otimes t) \circ (\rho \otimes \sigma) .$$

Next we show that <u>$U^*$ is an integral domain</u>. Let $g_1, \ldots, g_n$ be elements of $U^*$ that vanish on $U_o = F$ and are such that their restrictions to $L$ constitute a basis for $L^*$. There exists a (dual) basis $x_1, \ldots, x_n$ of $L$ such that $g_i(x_j) = \delta_{ij}$, $i, j = 1, \ldots, n$. Then every monomial of degree $> p$ in the $g_i$ vanishes on the subspace, $U_p$, of $U$ which consists of all elements that can be written as "polynomials" of degree $\leq p$ in elements of $L$. This follows easily from the definition of the multiplication by induction on $p$. Further, one can also see by induction that

$$(g_1^{q_1} \cdots g_n^{q_n})(x_1^{e_1} \cdots x_n^{e_n}) = \delta_{q_1,e_1} \cdots \delta_{q_n,e_n} \, e_1! \cdots e_n! .$$

Hence every element of $U^*$ coincides on $U_p$ with a unique polynomial of degree $\leq p$ in the $g_i$. This gives an algebra isomorphism of $U^*$ onto the algebra of formal power series in $n$-variables (corresponding to the $g_i$). In particular, it follows that $U^*$ is an integral domain.

<u>Notation:</u> Let $\rho$ be a representation of a Lie algebra $L$ over a field of characteristic $0$ and let $M$ be the representation space for $\rho$.

Put $E = \mathrm{Hom}_F(M, M)$ and denote by $P$ the algebra of polynomial functions on $E$. Let $S_\rho$ be the subalgebra of $R$ that is generated by the "constants" and the representative functions associated with $\rho$.

[$f$ is a constant in $R$ if and only if $f(LU) = 0$. Hence the map $f \dashrightarrow f(1)$ is an isomorphism of the constant functions onto $F$. Moreover, multiplication by a constant $f$ in $U^*$ is the same as multiplication by $f(1)$.]

If $f$ is any function on $E$ and $e$ is in $E$ then, as before, we define the left (right) translate of $f$ by $e$ so that

$$(e.f)(x) = f(xe) \quad ((f.e)(x) = f(ex))$$

for all $x$ in $E$.

Now $U^*$ is a left unitary $U$-module such that $(u.f)(u') = f(u'u)$ for all $u, u' \in U$ and all $f$ in $U^*$. Thus if $\sigma$ is any representation of $U$ with representation space $M_\sigma$ and if $\tau$ is in $E(M_\sigma)^*$, $u$ in $U$, we have

$$u.(\tau \circ \sigma) = (\sigma(u).\tau) \circ \sigma ,$$

so that $R$ is a $U$-submodule of $U^*$.

If $e$ is in $E$, denote by $D_e$ the derivation of $P$ that coincides with left translation by $e$ on $E^*$. Clearly, such a $D_e$ commutes with every right translation on $P$. We regard $P$ as a left unitary $U$-module such that the endomorphism of $P$ corresponding to $x$ in $L$ is $D_{\rho(x)}$, and we denote this operation of $U$ on $P$ be $p \dashrightarrow u(p)$ for $u$ in $U$ and $p$ in $P$. The map $t \dashrightarrow t \circ \rho$ from $E^*$ to $S_\rho$ extends to a unitary algebra epimorphism of $P$ onto $S_\rho$ which we denote by $p \dashrightarrow p'$. We assert now that the map $p \dashrightarrow p'$ is also a $U$-module homomorphism.

We show first that for $x$ in $L$, the map $f \dashrightarrow x.f$ on $U^*$ is a derivation. In fact, if $f$ and $g$ are elements of $U^*$, $x$ is in $L$, $u$ in $U$ and $du = \sum a_i \otimes b_i$, we have

$$(x.(fg))(u) = fg(ux) = f \otimes g(dudx)$$

$$= f \otimes g \left(\sum a_i \otimes b_i\right)(1 \otimes x + x \otimes 1)$$

$$= \sum \left(f(a_i)\, g(b_i x) + f(a_i x)\, g(b_i)\right)$$

$$= (f(x.g) + (x.f)g)(u) \quad .$$

(From this it follows that $S_\rho$ is a U-submodule of $R$.)

For fixed $x$ in $L$, define the F-linear map $f: P \dashrightarrow S_\rho$ by $f(p) = (x(p))' - x.p'$ for all $p$ in $P$. Then $f(pg) = p'f(q) + f(p)q'$ for all $p, q \in P$. Hence, in order to show that $f = 0$, it suffices to show that $f(p) = 0$ for every $p$ in $E^*$. Now if $p$ is in $E^*$ and $x$ is in $L$ then

$$f(p) = (x(p))' - x.p' = (\rho(x).p)' - x.p'$$

$$= \rho(x).p \circ \rho - x.(p \circ \rho) = 0 \quad .$$

This proves the assertion.

Let $Q$ be the kernel of the epimorphism $p \dashrightarrow p'$. Q is called the ideal associated with $\rho$.

Now we show that the set $G$ of all automorphisms of $M$ that are zeros of $Q$ is a group. Let $H$ be the group of all automorphisms of $M$ such that $Q.h = Q$. If $p$ is in $P$, it follows from the definition of the map $p \dashrightarrow p'$ that $p'(1)$ is the value taken by $p$ at the identity automorphism $I$ of $M$. Hence, if $p$ is in $Q$, then $p(I) = 0$. Thus if $h$ is in $H$, $p$ in $Q$, then $p.h$ is in $Q$ so that $(p.h)(I) = p(h) = 0$. Thus $h$ is in $G$, hence $H \subset G$.

On the other hand, since $p \dashrightarrow p'$ is a U-homomorphism, Q is U-stable, i.e., if u is in U, q in Q, then u(q) is in Q. Let g be in G, q in Q and u in U. Then

$$(q.g)'(u) = u.(q.g)'(1) = (u(q.g))'(1) = (u(q).g)'(1)$$
$$= (u(q).g)(I) = u(q)(g) = 0 .$$

Therefore q.g is in Q whence $Q.g \subset Q$. Hence, since translations also preserve degrees and g is an automorphism, we get $Q.g = Q$, i.e., g is in H. Therefore $G \subset H$, so that $G = H$.

Let T be any group of automorphisms of M, A the ideal associated with T and suppose $\rho(L) \subset T^{\circ}$. Then, for every u in U and every p in A, u(p) is in A. Hence $(u(p))(I) = 0$ and $(u(p))'(1) = 0$, i.e., $(u.p')(1) = 0$ or $p'(u) = 0$. Hence p is in Q whence $A \subset Q$. Thus $G \subset T$ and we conclude that $G \subset G_{\rho(L)}$. Now we show that $G = G_{\rho(L)}$.

We recall that exp(te) was defined as the element of $E \otimes_F t$ such that $\lambda(\exp(te)) = \sum_{n=0}^{\infty} \frac{\lambda(e^n)}{n!} t^n$ for every $\lambda$ in $E^*$. Further, we have identified P with the corresponding F-algebra of maps: $E \otimes_F F\{t\} \longrightarrow F\{t\}$. If f(t) is in $F\{t\}$ and p is in P, we define f(t)p by $(f(t)p)(z) = f(t)p(z)$ for every z in $E \otimes_F F\{t\}$. Similarly, we interpret the formal power series $\exp(tD_e) = \sum_{n=0}^{\infty} \frac{t^n}{n!} D_e^n$ as a map from P to $F\{t\}$ P such that, formally,

$$(\exp(tD_e))(p) = \sum_{n=0}^{\infty} \frac{t^n}{n!} D_e^n(p) .$$

Actually, this last formal power series is understood to be that element w of $F\{t\}$ P which satisfies

$$\mu(w) = \sum_{n=0}^{\infty} \frac{\mu(D_e{}^n(p))}{n!} t^n$$

for every $\mu$ in $P^*$. That this condition uniquely defines an element of $F\{t\}P$ follows from the fact that with $P_d$ = polynomials of degree $\leqq d$ in elements of $E^*$, $P_d$ is stable under $D_e$ and is of finite dimension over $F$. Now it is easy to verify that $\exp(tD_e)$ is a homomorphism and coincides with the translation which is defined in $F\{t\}P$ by $\exp(te)$, i.e., $\exp(te).p = \exp(tD_e)(p)$ for every $p$ in $P$. Therefore, if $e = \rho(x)$ with $x$ in $L$, and if $p$ is in $Q$,

$$p(\exp(te)) = \exp(tD_e)(p)\{I\} = \sum_{n=0}^{\infty} \frac{1}{n!} p'(x^n)t^n = 0 ,$$

since

$$D_e(p)\{I\} = x(p)\{I\} = (x(p))'(1) = x.p'(1) = p'(x) .$$

Let $Q_e$ be the ideal associated with $G_e$. We have just seen that $Q \subset Q_e$. Thus $G_e \subset G$. Hence $e$ is in $(G_e)^\cdot \subset G^\cdot$. Thus $\rho(L) \subset G^\cdot$. This means that $G = G_{\rho(L)}$. The above, applied to $T = G_{\rho(L)}$ shows that the ideal associated with $G_{\rho(L)}$ is contained in $Q$ and hence coincides with $Q$.

Def. An algebraic group is called irreducible if its associated ideal is prime.

We have proved

Theorem 2. Let $\rho$ be a finite-dimensional representation of $L$ with representation space $M$ over a field of characteristic 0. Let $Q$ be the ideal associated with $\rho$. Then the set $G$ of all automorphisms of $M$ that are zeros of $Q$ is an irreducible algebraic group and $\rho(L) \subset G^\cdot$. Moreover, $G$ is contained in every algebraic group of automorphisms of $M$ whose Lie algebra contains $\rho(L)$, i.e., $G = G_{\rho(L)}$. Further, $Q$ is the ideal of polynomial functions associated with $G$.

Corollary. The Lie algebra $G^\circ$ of $G$ is the algebraic hull of $\rho(L)$ and consists of all $e$ in $E$ for which $D_e(Q) \subset Q$. The ideal associated with the identity representation of $\rho(L)$ coincides with $Q$.

Proof: The first part is already done, so we need only check the last statement. Let $Q'$ be the ideal associated with the identity representation of $G^\circ$. By Theorem 2, $Q'$ is the ideal of all polynomial functions which vanish on the smallest algebraic group $H$ whose Lie algebra contains $G^\circ$. Since $\rho(L) \subset G^\circ$ it follows that $G \subset H$. Hence $Q' \subset Q$. Now suppose $q$ is in $Q$. Then $u(q)$ is in $Q$ for every $u$ in the universal enveloping algebra of $G^\circ$. In particular, $u(q)\{I\} = 0$ so that $u(q)'(1) = 0$, i.e., $q'(u) = 0$. Thus $q$ is in $Q'$ and $Q \subset Q'$. Q.E.D.

Let $L$ be a Lie algebra with universal enveloping algebra $U$ and let $\rho$ be a representation of $L$ with representation space $M$. $\rho$: $L \longrightarrow E = \mathrm{Hom}_F(M, M)$. We have defined a U-module structure on $P$, the algebra of polynomial functions on $E$, such that the map $P \longrightarrow S_\rho$ is a U-module homomorphism. Replacing left translations by right translations throughout, we define the structure of a right U-module on $P$ so that the same map $P \longrightarrow S_\rho$ is a right U-module homomorphism. The right U-operations on $P$ commute with the left and the same is true for $S_\rho$. Moreover, for every $e$ in $E$, $D_e$ commutes with the right U-operations on $P$. Suppose $D_e(Q) \subset Q$. Then $D_e$ induces a derivation on $P/Q$ and hence on $S_\rho$. This derivation of $S_\rho$ is denoted by $D_e'$. $D_e'$ commutes with the right translations on $S_\rho$. Let $S$ be any subalgebra of $R$ containing the constants and stable under right translations. Then a derivation of $S$ is called proper if it annihilates the constants and commutes with the right

translations. Thus $D_e'$ is a proper derivation of $S_\rho$. The map $e \longrightarrow D_e'$ is a homomorphism of $G'$ (the algebraic hull of $\rho(L)$) into the Lie algebra of all proper derivations of $S_\rho$. This map is an isomorphism onto, for, if $D_e' = 0$ then $D_e(P) \subset Q$. In particular, $D_e(p)$ is in $Q$ for all $p$ in $E^*$. Hence $0 = D_e(p)\{I\} = p(e)$ for all $p$ in $E^*$. Hence $e = 0$ and therefore the map is a monomorphism. Now let $D$ be a proper derivation of $S_\rho$. Then the map $p \longrightarrow D(p')(1)$ is a linear function on $E^*$. Hence there exists $e$ in $E$ such that $d(p')(1) = p(e)$ for every $p$ in $E^*$. Thus $D(p')(1) = D_e(p)\{I\}$ for every $p$ in $E^*$. This extends to hold for every $p$ in $P$ since the maps $p \longrightarrow D(p')(1)$ and $p \longrightarrow D_e(p)\{I\}$ are differentiations. Hence it follows that $e$ is in $G$. Hence $D_e'$ is defined and $D_e'(p') = D_e(p)'$ for every $p$ in $P$. Moreover, $D_e'(p')(1) = D_e(p)'(1) = D_e(p)\{I\} = D(p')(1)$. Since both $D$ and $D_e'$ commute with right $U$-translations, it follows that $D_e' = D$. Thus our map is an epimorphism.

Now $\rho(L)$ is an algebraic Lie algebra if and only if $(L) = G'$. Therefore we have

Theorem 3. The Lie algebra $\rho(L)$ is algebraic if and only if every proper derivation of $S_\rho$ is left translation by an element of $L$.

As before, we denote the algebra of representative functions on $L$ by $R$.

Lemma 2. Let $A$ be a subspace of $R$ that is stable under the right translations and let $B$ be a subspace of $A$ that is stable under the left translations. Then every linear map of $A$ into $U^*$ that commutes with the right translations maps $B$ into itself.

Proof: Let b be in B and let [b] denote the subspace of B spanned by the left translates of B . Since b is in R, [b] is finite dimensional. Hence we can find a basis $b_1, \ldots, b_n$ of [b] and elements $u_1, \ldots, u_n$ in U such that $b_i(u_j) = \delta_{ij}$ . Then for every u in U, we have

$$u.b = \sum_{i=1}^{n} b(u_i u) b_i \quad ;$$

this is easily verified by applying both sides to $u_j$ for $j = 1, \ldots, n$ . Evaluating at an element v in U we find

$$b(vu) = \sum_{i=1}^{n} b(u_i u) b_i(v) \quad .$$

Hence

$$b.v = \sum_{i=1}^{n} b_i(v)\, b.u_i \quad .$$

Now let $\lambda$ be a linear map: A ---> $U^*$ commuting with right translations. Then

$$\lambda(b).v = \sum_{i=1}^{n} b_i(v)\, \lambda(b).u_i \quad .$$

Evaluate at 1 in U :

$$\lambda(b)(v) = \sum_{i=1}^{n} \lambda(b)(u_i)\, b_i(v) \quad .$$

Therefore

$$\lambda(b) = \sum_{i=1}^{n} \lambda(b)(u_i)\, b_i$$

is in B.

Prop 1. Let S be a subalgebra of R that contains the constants and is stable under right translations. If D is a proper derivation of S, define the differentiation D' of S into F such that $D'(s) = D(s)(1)$ . Then the map D ---> D' is a linear isomorphism of the space of all proper

derivations of S onto the space of all differentiations of S.

Proof: Let $\delta$ be a differentiation of S. Define a linear map $\delta^*$ of S into $U^*$ by $\delta^*(s)(u) = \delta(s.u)$ for all s in S and all u in U. Then $\delta^*$ commutes with right translations and we apply Lemma 1, with $A = B = S$, to obtain $\delta^*(S) \subset S$. Let $\phi$ be the multiplication in $U^*$, $\phi: U^* \otimes U^* \longrightarrow U^*$. Let us regard $U^* \otimes_F U^*$ as a right $U \otimes_F U$-module such that $(f \otimes g).(a \otimes b) = (f.a) \otimes (g.b)$ for all f, g in $U^*$ and a, b in U. Then if f, g are in $U^*$, u in U,

$$(fg).u = \phi((f \otimes g).du) \quad .$$

[To see this,

$$((fg).u)(v) = (fg)(uv) = f \otimes g(dudv) = ((f \otimes g).du)(dv) = \phi((f \otimes g)du)(v)$$

If f and g are in S,

$$\delta((f.a)(g.b)) = \delta(f.a)(b.g)(1)) + ((f.a)(1))\delta(g.b)$$
$$= \delta(f.a)\ g(b) + f(a)\ \delta(g.b)$$
$$= (\delta^* f \otimes g)(a \otimes b) + (f \otimes \delta^* g)(a \otimes b).$$

Hence, (writing $du = \sum a_i \otimes b_i$ in $U \otimes U$)

$$(\delta^*(f) \otimes g + f \otimes \delta^*(g))(du) = \sum \delta((f.a_i)(g.b_i))$$
$$= \sum \delta(\phi((f \otimes g).(a_i \otimes b_i))$$
$$= \delta(\phi((f \otimes g).du))$$
$$= \delta((fg).u) \quad ,$$

i.e.,

$$(\delta^*(f)g + f\delta^*(g))(u) = \delta^*(fg)(u) \quad .$$

Thus

$$\delta^*(f)g + f\,\delta^*(g) = \delta^*(fg) \quad ,$$

so that $\delta^*$ is a proper derivation of S. Clearly, $(\delta^*)^* = \delta$. Further, if D is any proper derivation of S, then $(D')^* = D$.

Theorem 3'. The Lie algebra $\mathcal{O}(L)$ is algebraic if and only if every differentiation of $S\rho$ is of the form $f \longrightarrow f(x)$ for some $x$ in L.

## 3. Elementary Theory of Algebraic Linear Groups.

Now we allow K be any field. If U and V are finite dimensional K-spaces we denote their direct sum by (U, V). P(U) will denote the algebra of polynomial functions on U. We identify P(U, V) with $P(U) \otimes_K P(V)$ by means of the map $\phi$: $P(U) \otimes_K P(V) \longrightarrow P(U, V)$ such that

$$\phi(p \otimes q)(u, v) = p(u)q(v) .$$

Theorem 4. Let A and B be subspaces of the vector spaces U and V. Let $\mathcal{A}$ and $\mathcal{B}$ be the ideals associated with A and B respectively. Then the ideal of P(U, V) associated with (A, B) "coincides" with $\mathcal{A} \otimes_K P(V) + P(U) \otimes_K \mathcal{B}$. If $\mathcal{A}$ and $\mathcal{B}$ are prime ideals, so is $\mathcal{A} \otimes_K P(V) + P(U) \otimes_K \mathcal{B}$. If A is the set of all zeros of $\mathcal{A}$ and B is the set of all zeros of $\mathcal{B}$ then (A, B) is the set of all zeros of $\mathcal{A} \otimes_K P(V) + P(U) \otimes_K \mathcal{B}$.

Proof: We denote $\mathcal{A} \otimes_K P(V) + P(U) \otimes_K \mathcal{B}$ by I. Write $P(U) = S + \mathcal{A}$ where S is a subspace of P(U) such that $S \cap \mathcal{A} = (0)$. Let f be in P(U, V) and suppose that the restriction of f to (A, B) is zero. Write $f = g + h$ with g in $S \otimes P(V)$, h in $\mathcal{A} \otimes P(V)$. Then g still vanishes on (A, B). Write $g = \sum s_i \otimes q_i$ with the $s_i$ being linearly

independent elements of $S$ and $q_i$ in $P(V)$. Then

$$\sum s_i(a)\, q_i(b) = 0$$

for all $(a, b)$ in $(A, B)$. Hence, the element $\sum q_i(b)s_i$ of $P(U)$ is zero on $A$. Hence $\sum q_i(b)s_i$ is in $\mathcal{O}$ and therefore

$$\sum q_i(b)s_i = 0 .$$

Thus $q_i(b) = 0$ whence $q_i$ is in $\mathcal{L}$. Thus $g$ is in $P(U) \otimes \mathcal{L}$ whence $f$ is in $I$.

Now suppose that $\mathcal{O}$ and $\mathcal{L}$ are prime ideals and that $f$, $k$ are elements of $P(U) \otimes P(V)$ such that $fk$ is in $I$ but $k$ is not in $I$. Write $f = g+h$ with $g$ in $S \otimes P(V)$ and $h$ in $\mathcal{O} \otimes P(V)$. Since $k \notin I$, there exists $(a,b)$ in $(A, B)$ such that $k(a,b) \neq 0$. Consider the polynomial function on $U$: $u \longrightarrow g(u,b)\, k(u,b)$. This polynomial function is $0$ on $A$ and hence belongs to $\mathcal{O}$. On the other hand, the function $u \longrightarrow k(u,b)$ is not in $\mathcal{O}$ so that the function $u \longrightarrow g(u,b)$ is in $\mathcal{O}$. Write $g = \sum s_i \otimes q_i$ with the $s_i$ (linearly independent) elements of $S$ and $q_i$ in $P(V)$. The polynomial function $u \longrightarrow g(u,b)$ is $\sum q_i(b)\, s_i$. Hence $q_i(b) = 0$ for each $i$. This holds for every $b$ in $\mathcal{L}$ for which there is an $a$ in $\mathcal{O}$ with $k(a,b) \neq 0$. Hence the polynomial function $(u,v) \longrightarrow k(u,v)\, q_i(v)$ is $0$ on $(A, B)$. Hence the polynomial function $v \longrightarrow k(a,v)\, q_i(v)$ is in $\mathcal{L}$. Thus, as before, $q_i$ is in $\mathcal{L}$ for each $i$ and therefore $g$ is in $P(U) \otimes \mathcal{L}$. Therefore $I$ is a prime ideal.

Now suppose that $A$ and $B$ are the sets of all zeros of $\mathcal{O}$ and $\mathcal{L}$ respectively and let $(u,v)$ be an element of $I$. Then, for every $p$ in $\mathcal{O}$,

$$0 = (p \otimes 1)(u,v) = p(u) .$$

It follows that $u$ is in $\mathcal{O}$. Similarly, one shows that $v$ is in $\mathcal{L}$. This completes the proof.

Let $V$ be a $K$-space, $E = \mathrm{Hom}_K(V, V)$ and let $\mu: (E, E) \longrightarrow E$ denote ordinary multiplication in $E$. For every $p \in P(E)$, $p \circ \mu$ is in $P(E, E)$. In fact, it suffices to prove this when $p$ is in $E^*$. Let $(\lambda_i)$ be a basis for $E^*$. Then for every $e$ in $E$, $p.e = \sum p_i(e)\, \lambda_i$. If $e_1$ is in $E$, $(p.e)(e_1) = \sum p_i(e)\, \lambda_i(e_1)$, i.e.,

$$p(ee_1) = \sum p_i(e)\ \lambda_i(e_1) .$$

Therefore,

$$p \circ \mu = \sum (p_i \otimes 1)(1 \otimes \lambda_i) .$$

Theorem 5. Let $A$ be a non-empty multiplicatively closed set of automorphisms of a finite-dimensional space $V$ and let $\mathcal{O}$ be the associated ideal in $P(E)$. Let $G$ be the set of all automorphisms of $V$ that are zeros of $\mathcal{O}$. Then $G$ is an algebraic group and its associated ideal is $\mathcal{O}$. An automorphism of $V$ is in $G$ if and only if $e.\mathcal{O} \subset \mathcal{O}$ (whence $e.\mathcal{O} = \mathcal{O}$).

Proof: Since $AA \subset A$, $p \circ \mu$ vanishes on $(A, A)$ for every $p$ in $\mathcal{O}$. By Theorem 4, it follows that $\mathcal{O} \circ \mu \subset \mathcal{O} \otimes P(E) + P(E) \otimes \mathcal{O}$. Now suppose $e$ is in $G$ and $p$ in $\mathcal{O}$. Then

$$(e.p)(x) = p(xe) = p \circ \mu(x, e) .$$

Hence $e.p$ is 0 on $A$ whence $G.\mathcal{O} \subset \mathcal{O}$. Thus $e.\mathcal{O} = \mathcal{O}$ for every $e$ in $G$.

Let $1$ be the identity element of $E$, $p$ be in $\mathcal{O}$ and $e$ in $G$. $(e.p)(1) = p(e) = 0$. Hence $1$ is in $G$. Now suppose that $e.\mathcal{O} \subset \mathcal{O}$ where $e$ is an automorphism (so that actually $e.\mathcal{O} = \mathcal{O}$). Let $p$

be an element of $\mathcal{A}$. Then $p(e) = (e.p)(1) = 0$ and therefore $e$ is in $G$. Thus $G$ is the set of all automorphisms $e$ of $V$ for which $e.\mathcal{A} \subset \mathcal{A}$ ( = the set of all automorphisms $e$ for which $e.\mathcal{A} = \mathcal{A}$ ) and therefore $G$ is an algebraic group. Let $\mathcal{L}_G$ be the ideal associated with $G$. Then $\mathcal{A} \subset \mathcal{L}_G$ by the definition of $G$. On the other hand, $G \supset A$ so that $\mathcal{A} \subset \mathcal{L}_G$. Therefore $\mathcal{A} = \mathcal{L}_G$. Q. E. D.

Now we assume $K$ infinite again in order to identify the polynomial functions on $E$ with the symmetric algebra over $E^*$.

Theorem 6. Let $G$ be an algebraic group of automorphisms of the finite-dimensional $K$-space $V$ and let $\mathcal{A}$ be its associated ideal. Then there exists one and only one irreducible subgroup $G_1$ of finite index in $G$. $G_1$ is normal in $G$. If $p$ and $q$ are elements of $P(E)$ such that $q(1) \neq 0$ and $pq$ is in $\mathcal{A}$, then $p$ is in the ideal $\mathcal{A}_1$ associated with $G_1$. Further, there is a single polynomial function $p_1$ such that $p_1(1) \neq 0$ and such that

$$\mathcal{A}_1 = \{ p \mid p \text{ in } P(E),\ pp_1 \text{ is in } \mathcal{A} \}.$$

Proof: Let $\mathcal{A}_1$ be the set of all $p$ in $P(E)$ for which there exists $p'$ in $P(E)$ with $p'(1) \neq 0$ and $pp'$ in $\mathcal{A}$. Clearly $\mathcal{A}_1$ is an ideal. Every ideal of $P(E)$ has a finite ideal basis so we write

$$\mathcal{A}_1 = P(E)q_1 + \ldots + p(E)q_h$$

with $q_1, \ldots, q_h$ in $\mathcal{A}_1$. Choose, for each $i$, $q_i'$ in $P(E)$ such that $q_i'(1) \neq 0$, $q_i q_i'$ is in $\mathcal{A}$, and put $p_1 = q_1' \ldots q_h'$. Then $p_1(1) \neq 0$ and $\mathcal{A}_1$ is the set of all $p$ in $P(E)$ such that $pp_1$ is in $\mathcal{A}$. Let $G_1$ be the set of all automorphisms of $V$ that are zeros of $\mathcal{A}_1$. Clearly

$\mathcal{O}_1 \subset \mathcal{O}$ so that $G_1 \subset G$. Also, 1 is in $G_1$. More generally, if e is in G and $p_1(e) \neq 0$ then e is in $G_1$. Now suppose that p is in P(E) and that p is zero on $G_1$. Then $pp_1$ is in $\mathcal{O}$ so that p is in $\mathcal{O}_1$. Hence $\mathcal{O}_1$ is the ideal associated with $G_1$.

Now suppose that p is in $\mathcal{O}_1$, e in G and $e_1$ in $G_1$, and consider $p(ee_1)p_1(e)$. We have $pp_1$ in $\mathcal{O}$, from which it follows that $(p.e)(p_1.e)$ is in $\mathcal{O}$. If $p_1(e) \neq 0$, i.e., $(p_1.e)(1) \neq 0$, this implies that p.e is in $\mathcal{O}_1$, whence $p(ee_1) = 0$. Hence $p(ee_1)p_1(e) = 0$ and so $(e_1.p)p_1$ is in $\mathcal{O}$, i.e., $e_1p$ is in $\mathcal{O}_1$. Hence $G_1G_1 \subset G_1$. Now, by Theorem 5, it follows that $G_1$ is an algebraic group.

To see that $G_1$ is irreducible, take p, q in P(E) such that pq is in $\mathcal{O}_1$ and q not in $\mathcal{O}_1$. Choose e in $G_1$ such that $q(e) \neq 0$. Then $(e.(pq))p_1 = (e.p)(e.q)p_1$ is in $\mathcal{O}$. But $((e.q)p_1)(1) = q(e)p_1(1) \neq 0$. Therefore e.p is in $\mathcal{O}_1$ and hence p is in $\mathcal{O}_1$. Therefore $\mathcal{O}_1$ is a prime ideal, i.e., $G_1$ is irreducible.

Consider the ideal generated by all polynomials of the form $e.p_1$ with e in G. There exists a finite set $e_1, \ldots, e_s$ of elements of G such that $e.p_1$ is in $P(E)e_1.p_1 + \ldots + P(E)e_s.p_1$ for every e in G. If e is in G then $(e.p_1)(e^{-1}) = p_1(1) \neq 0$. Therefore there exists an i such that $(e_i.p_1)(e^{-1}) \neq 0$, i.e., that $p_1(e^{-1}e_i) \neq 0$. As was seen above, this means that $e^{-1}e_i$ is in $G_1$. Hence $G = \bigcup_{i=1}^{s} e_i G_1$ and therefore $G_1$ is of finite index in G.

Let H be any irreducible algebraic subgroup of G that is of finite index in G. Let h be the ideal associated with H. Then $\mathcal{O} \subset h$ and $p_1$ is not in h. If p is in $\mathcal{O}_1$, then $pp_1$ is in $\mathcal{O} \subset h$ and so p is in h. Thus $\mathcal{O}_1 \subset h$.

Let $H, He_1, \ldots, He_n$ be all of the distinct cosets of $H$ in $G$. Then $e_i^{-1}$ is not in $H$ and therefore there exists $q_i$ in $h$ such that $q_i(e_i^{-1}) \neq 0$. Put $q = \prod_{i=1}^{m} e_i^{-1} \cdot q_i$. By construction, $q(1) \neq 0$, but $q$ restricts to $0$ on $He_i$. Now let $p$ be in $h$. Then $pq$ is in $\mathcal{O}$ and therefore $p$ is in $\mathcal{O}_1$. Hence $h \subset \mathcal{O}_1$ so that $h = \mathcal{O}_1$. Thus $H = G_1$.

Let $e$ be in $G$ and consider $eG_1e^{-1}$. This is an irreducible algebraic subgroup of finite index (its associated ideal is $e\mathcal{O}_1e^{-1}$) and therefore $eG_1e^{-1} = G_1$. Thus $G_1$ is normal in $G$. Q.E.D.

Def. $G_1$ is called the <u>algebraic component of the identity in $G$</u> and the cosets of $G_1$ in $G$ are called the <u>algebraic components of $G$</u>.

<u>Theorem 7</u>. Let $G$ be a group of automorphisms of the finite-dimensional $K$-space $V$ and suppose that $G$ has a subgroup $H$ which is an algebraic group and is of finite index in $G$. Then $G$ is an algebraic group.

<u>Proof</u>: Let $\mathcal{O}$ be the ideal associated with $G$. Let $e$ be an automorphism of $V$ that is a zero of $\mathcal{O}$. Let $He_1, \ldots, He_n$ be all of the distinct cosets of $H$ in $G$. If $e$ is not in $G$, then no $ee_i^{-1}$ lies in $H$, $i = 1, \ldots, n$. Hence there exists $p_i$ in $P(E)$ such that $p_i$ restricts to zero on $H$ but $p_i(ee_i^{-1}) \neq 0$. Now put $p = \prod_{i=1}^{n} e_i^{-1} \cdot p_i$. Then $p$ is zero on $G$ and so $p$ is in $\mathcal{O}$. But then $p(e) = 0$ which is a contradiction. Q.E.D.

<u>Corollary</u>. Let $G$ be an algebraic group of automorphisms of $V$ and let $G_1$ be the component of the identity in $G$. Then a subgroup $H$ of $G$ is algebraic if and only if $H \cap G_1$ is algebraic.

<u>Proof</u>: If $H$ is algebraic, so is $H \cap G_1$. On the other hand, $H \cap G_1$ has finite index in $H$ because $G_1$ has finite index in $G$. Hence if $H \cap G_1$ is algebraic, $H$ is algebraic by Theorem 7.

4. Rational Functions.

Let U be a vector space over K, H any non-empty subset of U.

Def. A polynomial function on H is the restriction to H of a polynomial function on U.

P(H) will denote the algebra of all polynomial functions on H.

Def. A rational function on H is a map f of a non-empty subset $H_f$ of H into K such that

(1) For every x in $H_f$, there exists p in P(H) such that $p(x) \neq 0$ and pf is a polynomial function on $H_f$.

(2) If p is in P(H) and pf is a polynomial function on $H_f$ then every x in H such that $p(x) \neq 0$ belongs to $H_f$.

(3) There exists q in P(H), not a zero-divisor in P(H), such that qf is a polynomial function on $H_f$.

Let T be the set of all non-zero-divisors of P(H). We define the K-algebra R(H) as the algebra of quotients $P(H)_T$, i.e., the algebra of equivalence classes of pairs (p,t), p in P(H), t in T where $(p,t) \sim (p', t')$ means $pt' = p't$. P(H) may be identified with a subalgebra of R(H).

Every $\alpha$ in R(H) defines a rational function $f_\alpha$ on H as follows: $H_{f_\alpha}$ is the set of all x in H for which there exists (a, b) in (P(H), P(H)) and (p,t) in $\alpha$ such that $at = pb$ and $b(x) \neq 0$. We claim that the element $a(x)/b(x)$ of K depends only on x and $\alpha$.

Suppose (a', b') and (p', t') was another choice for x. Then $(a'b - ab')tt' = a'btt' - ab'tt' = p'b'bt - pbb't = (p't - pt')bb' = 0$. Therefore, since tt' is not a zero-divisor, $a'b - ab' = 0$. Hence $a(x)/b(x) = a'(x)/b'(x)$. We define $f_\alpha(x) = a(x)/b(x)$.

Now we verify that the pair $(f_\alpha, H_\alpha)$ satisfy conditions (1), (2), and (3).

(1) With x, a, b as above we claim that $bf_\alpha = a$ on $H_{f_\alpha}$. Indeed, let y be in $H_{f_\alpha}$ and choose a', b', p', t' in P(H) such that $a't' = p'b'$, $b'(y) \neq 0$. Then $b'(y)f_\alpha(y) = a'(y)$. Further, treating $(ab' - ba')tt'$ exactly as above, we see that $ab' - ba' = 0$. Hence, $b(y)b'(y)f_\alpha(y) = b(y)a'(y) = b'(y)a(y)$ whence $b(y)f_\alpha(y) = a(y)$, i.e., $bf_\alpha = a$ on $H_{f_\alpha}$.

(2) Suppose a, b in P(H) and $bf_\alpha = a$ on $H_{f_\alpha}$. Let p, t be in $f_\alpha$. Then, by the proof of (1), $tf_\alpha = p$ on $H_{f_\alpha}$. Hence, $pb = btf_\alpha = ta$ on $H_{f_\alpha}$ and hence everywhere because $t(x) \neq 0$ implies x in $H_{f_\alpha}$. Since t is not a zero-divisor in P(H), this gives $pb = ta$. Hence, if x is in H and $b(x) \neq 0$, then x is in $H_f$.

(3) Let (p,t) be in $\alpha$. Then, by the proof of (1), $tf_\alpha = p$ on $H_{f_\alpha}$. Hence (3) is satisfies with $q = t$.

Conversely, if f is a rational function on H, then by (3), there exists a non-zero-divisor q in P(H) and an element p in P(H) such that $qf = p$ on $H_f$. Let $\alpha$ be the element of R(H) such that (p,q) is in $\alpha$. Now we show that $f_\alpha = f$.

Take x in $H_f$. Then there exist a, b in P(H) such that $bf = a$ on $H_f$ and $b(x) \neq 0$ by (1). Now consider $(aq = pb)q$. If y is in H and $q(y) \neq 0$ then y is in $H_f$ by (2) and $a(y)q(y) = b(y)f(y)q(y) = b(y)p(y)$. Hence $(aq = bp)q = 0$. Since q is not a zero-divisor, this gives $aq = bp$. Hence x is in $H_{f_\alpha}$ and $f_\alpha(x) = \frac{a(x)}{b(x)} = f(x)$. Now let z belong to $H_{f_\alpha}$. Then there exist a, b in P(H) such that $b(z) \neq 0$ and $aq = pb$. We claim that

$bf = a$ on $H_f$. We have already shown that $H_f \subset H_{f_\alpha}$ and that $f_\alpha$ coincides with $f$ on $H_f$. From the proof of (1) above, we know that $bf_\alpha = a$. Hence $bf = a$ on $H_f$. Hence, by (2), $x$ is in $H_f$. Thus $H_f = H_{f_\alpha}$ and $f = f_\alpha$.

Thus the set of all rational functions on $H$ is in one-to-one correspondence with the elements of $R(H)$ and therefore inherits the structure of a K-algebra.

Def. A subset $S$ of $H$ is called algebraically dense in $H$ if there exists a non zero-divisor $q$ in $P(H)$ such that $q(x) \neq 0$ implies $x$ is in $S$.

Lemma 3. Let $f$ and $g$ be rational functions on $H$ and suppose there exists a dense subset $S$ of $H$ such that $f(x) = g(x)$ for all $x$ in $S \cap H_f \cap H_g$. Then $f = g$.

Proof: There exists a non zero-divisor $s$ in $P(H)$ such that $sf = u$ on $H_f$ where $u$ is in $P(H)$, $sg = v$ on $H_g$ where $v$ is in $P(H)$ and also $f(x) = g(x)$ whenever $s(x) \neq 0$. (Find a non zero-divisor for each of these conditions separately and put $s$ = the product.)

Suppose $a$, $b$, $a^*$, $b^*$ are elements of $P(H)$ such that $bf = a$ on $H_f$, $b^*g = a^*$ on $H_g$. Now since $sf = u$ on $H_f$ and $bf = a$ on $H_f$, $bu = sbf = sa$ on $H_f$. By conditions (2) and (3) for rational functions, there is a non zero-divisor $q$ in $P(H)$ such that every $x$ in $H$ for which $q(x) \neq 0$ belongs to $H_f$. Now $(bu - sa)q = 0$ and hence $bu = sa$. Similarly $b^*v = sa^*$. Since $u(x) = v(x)$ whenever $s(x) \neq 0$, it follows that $su = sv$. Hence, since $s$ is not a zero-divisor, $u = v$. $b^*as = bb^*u = b^*as$ whence $ba^* = b^*a$.

Hence, on $H_g$, $(bg - a)b^* = bb^*g - ab^* = ba^* - ab^* = 0$. Hence $b(x)g(x) = a(x)$ whenever $b^*(x) \neq 0$. But if $x$ is in $H_g$, $b^*$ may be chosen so that $b^*(x) \neq 0$. Hence $b(x)g(x) = a(x)$ for every $x$ in $H_g$, i.e., $bg = a$ on $H_g$. Now suppose $x$ is in $H_f$. Then we can choose the above $a$, $b$ in $P(H)$ such that $bf = a$ on $H_f$ and $b(x) \neq 0$. Since $bg = a$ on $H_g$, it follows that $x$ is in $H_g$ by condition (2). Thus $H_f \subset H_g$ and $f(x) = g(x)$ for all $x$ in $H_f$. Similarly $H_g \subset H_f$. Thus $H_f = H_g$ and $f = g$. Q.E.D.

As before, $H$ is a subset of a vector space $U$ and now let $V$ be another vector space.

Def. A map $\rho : H \dashrightarrow V$ is called a polynomial map if $\lambda \circ \rho$ is in $P(H)$ for every $\lambda$ in $V^*$. A rational map from $H$ to $V$ is a map $\rho$ of a dense subset $H\rho$ of $H$ into $V$ such that for every $\lambda$ in $V^*$, $\lambda \circ \rho$ is the restriction to $H\rho$ of a rational function $\rho_\lambda$ on $H$ and $H\rho = \bigcap_{\lambda \in V^*} H\rho_\lambda$.

Note that, since $H\rho$ is dense in $H$, it follows from Lemma 3 that $\rho_\lambda$ is uniquely determined by $\rho$ and .

Let $\lambda_1, \ldots, \lambda_n$ be a basis for $V^*$ and write $\rho_i$ for $\rho_{\lambda_i}$. Every element $\lambda$ of $V^*$ is a linear combination $\lambda = k_1\lambda_1 + \ldots + k_n\lambda_n$ with $k_1, \ldots, k_n \in K$ and $\rho_\lambda$ coincides with $k_1\rho_1 + \ldots + k_n\rho_n$ on $H\rho$. Since $H\rho$ is dense, the Lemma gives that $\rho_\lambda = k_1\rho_1 + \ldots + k_n\rho_n$ and hence $H\rho_\lambda \supset \bigcap_{i=1}^{n} H\rho_i$. (Note that it follows easily from our definitions that if $f$ and $g$ are any two rational functions on $H$ then $H_{f+g} \supset H_f \cap H_g$ and $H_{fg} \supset H_f \cap H_g$ and further, for every $x$ in $H_f \cap H_g$, $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. Moreover,

by the Lemma, f + g and fg are uniquely determined by these properties.)

On the other hand, the definition of rational map gives $H\rho_\lambda \subset \bigcap_{i=1}^{n} H\rho_i$. Therefore $H\rho_\lambda = \bigcap_{i=1}^{n} H\rho_i$ and $\rho^\lambda$ is given by $\rho(x) = \sum_{i=1}^{n} \rho_i(x)v_i$ where the $v_i$ are elements of V such that $\lambda_i(v_j) = \delta_{ij}$.

Thus $\rho$ determines an element $\sum \rho_i \otimes v_i$ of $R(H) \otimes_K V$.

Conversely, if $\alpha$ is in $R(H) \otimes_K V$, we have $\alpha = \sum f_i \otimes v_i$ with the $f_i$ in R(H) and the $v_i$ linearly independent in V. Then $\alpha$ determines a rational map $\rho_\alpha$: H ---> V such that $H\rho_\alpha = \bigcap_{i=1}^{n} Hf_i$ and $\rho_\alpha(x) = \sum f_i(x)v_i$ for all x in $H\rho_\alpha$.

This gives a one-to-one correspondence between rational maps: H ---> V and elements of $R(H) \otimes V$. We identify $R(H) \otimes V$ with the corresponding rational maps so that the rational maps become an R(H)-module.

Def. A rational representation of an algebraic group G is a representation of G which is also a rational map.

Theorem 8. Let G be an algebraic group of automorphisms of the K-space U. Let $\rho$ be a rational representation of G by automorphisms of another vector space V. Let H be an algebraic group of automorphisms of V. Then $\rho^{-1}(H)$ is an algebraic subgroup of G.

Proof: Let $\mathcal{L}$ be the ideal of P(E(H)) associated with $\rho^{-1}(H)$. Let B be the set of all automorphisms of U that are zeros of $\mathcal{L}$. By Theorem 5, B is an algebraic group with associated ideal $\mathcal{L}$. Let $\mathcal{O}$ be the ideal associated with G. Then $\mathcal{O} \subset \mathcal{L}$ whence $B \subset G$.

Now let b be in B and let q be a polynomial function on E(V) which is zero on H. Then $q \circ \rho$ is a rational function on G

and $q \circ \rho$ is zero on $\rho^{-1}(H)$. Now $q \circ \rho$ is defined at every point of $G$ so there exist $u_b$ and $v_b$ in $P(E(U))$ such that $v_b(b) \neq 0$ and $q \circ \rho(x) = \frac{u_b(x)}{v_b(x)}$ whenever $x$ is in $G$ and $v_b(x) \neq 0$. Then $u_b v_b$ is in $\mathfrak{L}$ so that $v_b(b)u_b(b) = 0$ and therefore $u_b(b) = 0$. Hence $q \circ \rho(b) = 0$. Since this holds for every $q$ in $E(V)$ which is zero on $H$, it follows that $\rho(b)$ is in $H$, i.e., $b$ is in $\rho^{-1}(H)$. Thus $B = \rho^{-1}(H)$. Q.E.D.

5. Extension of the Base Field.

Let $L$ be an arbitrary extension of our base field $K$. If $V$ is a finite-dimensional $K$-space, we shall write $V^L$ for $V \otimes_K L$ and identify $E(V)^L$ with $E(V^L)$. Also, every element of $E(V)^*$ can be extended uniquely to an element of $(E(V)^*)^L = (E(V)^L)^* = E(V^L)^*$. Hence we obtain a $K$-algebra monomorphism: $P(E(V)) \longrightarrow P(E(V^L))$. Identifying $P(E(V))$ with its image in $P(E(V^L))$ we write $P(E(V^L)) = (P(E(V))^L$.

Theorem 10. Let $G$ be an algebraic group of automorphisms of $V^L$. Then $G \cap E(V)$ is an algebraic group of automorphisms of $V$.

Proof: Let $\mathfrak{A}$ be the ideal associated with $G$ in $P(E(V^L))$. Let $(l_i)$ be a basis for $L$ over $K$. Then if $p$ is in $\mathfrak{A}$, write $p = \sum p_i \otimes l_i$ with $p_i$ in $P(E(V))$. Let $S$ be the set of all $p_i$ so obtained. Then $G \cap E(V)$ is the set of all automorphisms of $V$ which are zeros of $S$. Hence $G \cap E(V)$ is an algebraic group. Q.E.D.

Lemma 4. Let $A$ be a subset of a finite-dimensional $K$-space $U$ and let $\mathfrak{A}$ be the ideal associated with $A$. Then the ideal associated with $A$ in $P(U^L)$ is $\mathfrak{A}^L$. Furthermore, $\mathfrak{A}^L$ is prime if and only if $\mathfrak{A}$ is prime.

Proof: Recall that $P(U^L) = P(U)^L$. Let $p$ be in $P(U^L)$ and suppose $p(A) = 0$. Let $(l_i)$ be a basis for $L$ over $K$ and write $p = \sum p_i \otimes l_i$ with the $p_i$ in $P(U)$. Then, since the $l_i$ are linearly independent, it follows that the $p_i$ are in $\mathcal{O}$. Therefore the ideal of $P(U^L)$ associated with $A$ is $\mathcal{O}^L$.

Clearly $\mathcal{O}^L \cap P(U) = \mathcal{O}$. Hence if $\mathcal{O}^L$ is prime, so is $\mathcal{O}$. Now suppose that $\mathcal{O}$ is prime. Let $p$ and $q$ be elements of $P(U^L)$ such that $pq$ is in $\mathcal{O}^L$ and $q$ is not in $\mathcal{O}^L$. Write $p = \sum p_i \otimes l_i$ and $q = \sum q_i \otimes l_i$. Since $q$ is not in $\mathcal{O}^L$, there exists an index $j$ such that $q_j$ is not in $\mathcal{O}$. Now choose $a$ in $A$ such that $q_j(a) \neq 0$. Then $q(a) \neq 0$ and, hence, since $p(a)q(a) = 0$, $p(a) = 0$ whence $p_i(a) = 0$ for each $i$. Hence $p_i(a)q_j(a) = 0$ for all $a$ in $A$, i.e., $p_i q_j$ is in $\mathcal{O}$. Since $q_j$ is not in $\mathcal{O}$ it follows that $p_i$ is in $\mathcal{O}$ and hence that $p$ is in $\mathcal{O}^L$. Thus $\mathcal{O}^L$ is prime.

Theorem 11. Let $G$ be an algebraic group of automorphisms of a finite-dimensional $K$-space $V$. Let $G^L$ be the intersection of all algebraic groups of automorphisms of $V^L$ that contain $G$. Let $\mathcal{O}$ be the ideal associated with $G$ in $P(E(V))$. Then the ideal associated with $G^L$ in $P(E(V^L))$ is $\mathcal{O}^L$. Further, $G^L \cap E(V) = G$. Let $G_1$ be the component of the identity in $G$. Then $(G_1)^L$ is the component of the identity in $G^L$. If $e_i G_1$ are the distinct cosets of $G_1$ in $G$ then $e_i(G_1)^L$ are the distinct cosets of $(G_1)^L$ in $G^L$.

Proof: By the Lemma, $\mathcal{O}^L$ is the ideal associated with $G$ in $P(E(V^L))$. Let $G^1$ be the set of all automorphisms of $V^L$ that are zeros of $\mathcal{O}^L$. By Theorem 5, $G^1$ is an algebraic group and its associated ideal is $\mathcal{O}^L$. Since $G^1 \supset G$, $G^L \supset G^1$. On the other hand, $G^L \supset G$ and hence the

ideal associated with $G^L$ is contained in $\mathcal{O}^L$ . Therefore $G^1 \subset G^L$ . Hence $G^1 = G^L$ and its associated ideal is $\mathcal{O}^L$ .

By Theorem 10, $G^L \cap E(V)$ is an algebraic group. Let p be in $\mathcal{O}$ . Then p is in $\mathcal{O}^L$ and hence p is zero on $G^L$ . Since G is an algebraic group, it follows that $G \supset G^L \cap E(V)$ . On the other hand, it is obvious that $G \subset G^L \cap E(V)$. Hence $G = G^L \cap E(V)$ .

Let $\mathcal{O}_1$ be the ideal associated with $G_1$ . Then $\mathcal{O}_1$ is prime and, by the Lemma, $\mathcal{O}_1^L$ is prime. Since $\mathcal{O}_1^L$ is the ideal associated with $(G_1)^L$ , $(G_1)^L$ is irreducible. The sets $e_i(G_1)^L$ are contained in $G^L$. Suppose now that $s_i$ and $s_j$ are elements of $(G_1)^L$ such that $e_i s_i = e_j s_j$ . Then $e_j^{-1} e_i = s_j s_i^{-1}$ is in $(G_1)^L \cap E(V) = G_1$ . Hence $i = j$ and thus the sets $e_i(G_1)^L$ are distinct.

Let s be an automorphism of $V^L$ that belongs to none of the $e_i(G_1)^L$ . Then, for each i, there exists $p_i$ in $P(E(V))$ such that $p_i$ is zero on $(G_1)^L$ while $p_i(e_i^{-1}s) \neq 0$ . Since $G = \bigcup_{i=1}^{h} e_i G_1$ , the function $\prod_{i=1}^{h} p_i \cdot e_i^{-1}$ is zero on G and hence also on $G^L$ . Since it does not vanish at s, s is not in $G^L$. Therefore $G^L = \bigcup_{i=1}^{h} e_i(G_1)^L$ . Thus $(G_1)^L$ is irreducible and of finite index in $G^L$ so that $(G_1)^L = (G^L)_1$ . Q.E.D.

Let P(B) be the algebra of all polynomial functions on G. Let p be in P(G) then p is the restriction to G of an element q in P(E(V)). We have identified P(E(V)) with its image in $P(E(V^L))$ . In this sense, we get $q|_{G^L}$ is in $P(G^L)$ . If q and r are two elements of P(E(V)) which coincide on G, then $q|_{G^L} = r|_{G^L}$ because every element of $P(E(V^L))$ that is zero on G is also zero on $G^L$ . Thus we get a map $P(G) \longrightarrow P(G^L)$ and this map is a K-algebra monomorphism.

This map can be extended by L-linearity to a map $\phi$: $P(G)^L \longrightarrow P(G^L)$. Since the map $P(E(V))^L \longrightarrow P(E(V^L))$ is an epimorphism, it follows that $\phi$ is an epimorphism. Now suppose $p$ is in $P(G)^L$ and $\phi(p) = 0$. Then $p = \sum p_i \otimes \ell_i$ with the $\ell_i$ linearly independent and $p_i$ in $P(G)$. Take $x$ in $G$. Then

$$0 = \phi(p)(x) = \sum \ell_i p_i(x)$$

and hence $p_i(x) = 0$ for each $i$. Therefore $p_i = 0$ and thus $p = 0$. Thus $\phi$ is also a monomorphism and hence $\phi$ is an isomorphism.

Let $R(G)$ and $R(G^L)$ denote the algebras of rational functions on $G$ and $G^L$ respectively. If $q$ is in $P(G)$ and $q$ is not a zero-divisor of $P(G)$ then its canonical image in $P(G^L)$ is not a zero divisor. For, suppose $p = \sum p_i \otimes \ell_i$ is an element of $P(G^L)$ with the $\ell_i$ linearly independent and suppose $qp = 0$. Then $qp = \sum qp_i \otimes \ell_i = 0$. Hence each $qp_i = 0$ whence each $p_i = 0$ and therefore $p = 0$. Hence the isomorphism $P(G) \longrightarrow P(G^L)$ can be extended uniquely to a K-algebra monomorphism: $R(G) \longrightarrow R(G^L)$ and hence to an L-algebra homomorphism: $R(G)^L \longrightarrow R(G^L)$. It follows immediately that this is still a monomorphism. However, it is generally <u>not</u> an epimorphism.

As before, let $H$ be a subset of a vector space $V$.

<u>Def.</u> A subset $S$ of $H$ is called a <u>unicity set</u> in $H$ if the restriction map $P(H) \longrightarrow P(S)$ is a monomorphism.

<u>Lemma 5.</u> Let $S$ and $T$ be subsets of $H$. Suppose that $S$ is a unicity set in $H$ and that $T$ is dense in $H$. Then $S \cap T$ is still a unicity set in $H$.

<u>Proof:</u> Since $T$ is dense, there exists a non zero-divisor $q$ in $P(H)$ such that if $q(x) \neq 0$ for $x$ in $H$, then $x$ is in $T$. Now let $p$

be in $P(H)$ and suppose $p$ is zero on $S \cap T$. Then $pq$ is zero on $S$ and hence $pq = 0$ since $S$ is a unicity set. Thus, since $q$ is not a zero-divisor, $p = 0$ . Q.E.D.

Lemma 6. Let $f$ and $g$ be rational maps from $H$ to a vector space $W$ and suppose there exists a unicity set $S$ in $H$ such that $f(x) = g(x)$ for all $x$ in $S \cap H_f \cap H_g$ . Then $f = g$ .

Proof: For each $\lambda$ in $W^*$ consider the rational functions $f_\lambda$ and $g_\lambda$ on $H$ and argue on $f_\lambda - g_\lambda$ . Since $F_{f_\lambda - g_\lambda} \supset H_{f_\lambda} \cap H_{g_\lambda}$ and since $S \cap H_f \cap H_g$ is still a unicity set in $H$ by the previous lemma, it suffices to prove that if a rational function $f$ is zero on $S \cap H_f$ then $f = 0$ .

There exists a non zero-divisor $q$ in $P(H)$ and $p$ in $P(H)$ such that $qf = p$ on $H_f$ . $qf$ is zero on $S \cap H_f$; thus $p$ is zero on $S \cap H_f$ . If $q(x) \neq 0$ then $x$ is in $H_f$ and therefore $qp$ is zero on $H$. Hence $p = 0$ and hence $f = 0$ .

Prop.2. Let $S$ be a dense subset of an algebraic group $G$. Then $SS = G$.

Proof: $S^{-1}$ is still a dense subset of $G$. In fact, there is a non zero-divisor $p$ in $P(G)$ such that if $x$ is in $G$ and $p(x) \neq 0$ then $x$ is in $S$. Define $\bar{p}(x) = p(x^{-1})$ . Let $d$ be the determinant function on $G$. Then $d^n\bar{p}$ is in $P(G)$ for $n$ large enough. Also $d^n\bar{p}$ is not a zero-divisor in $P(G)$. In fact, suppose that $q$ is in $P(G)$ and that $d^n\bar{p}q = 0$ . Then $(\bar{d})^n p\bar{q} = 0$ . But $\bar{d} = \frac{1}{d}$ so that we may conclude that $d^n p\bar{q} = 0$ for all $n$. Taking $n$ so large that $d^n\bar{q}$ is in $P(G)$ we conclude $d^n\bar{q} = 0$ whence $q = 0$ .

If $(d^n\bar{p})(x) \neq 0$ , then $p(x^{-1}) \neq 0$ so $x^{-1}$ is in $S$ whence $x$ is in $S^{-1}$ . Therefore $S^{-1}$ is dense in $G$. Take $e$ in $G$. Then, since $S^{-1}$ is dense and since the map $p \dashrightarrow e.p$ is an auto-

morphism of $P(G)$, it follows that $S^{-1}e$ is still dense in $G$. Hence $S^{-1}e \cap S$ is dense and, in particular, $S^{-1}e \cap S \neq \emptyset$. Take $s_1$ in $S^{-1}e \cap S$. Then $s_1 = s_2^{-1}e$ for some $s_2$ in $S$, i.e., $e = s_2 s_1$. Q.E.D.

Theorem 12. Let $G$ be an algebraic group of automorphisms of a finite-dimensional $K$-space $V$ and let $\rho$ be a rational representation of $G$ by automorphisms of a finite-dimensional $K$-space $U$. Let $H$ be the algebraic group hull of $\rho(G)$ and let $L$ be an extension field of $K$. Then there exists one and only one rational representation $\rho^L$ of $G^L$ by automorphisms of $U^L$ that extends $\rho$. Further, the algebraic group hull of $\rho^L(G^L)$ is $H^L$.

Proof: $\rho$ can be extended to a rational map $\rho^L: G^L \dashrightarrow E(U^L)$. Put $R = (G^L)_{\rho^L}$. Evidently $G \subset R$. For $x$ in $G^L$, let $\tau_x$ be the polynomial map: $G^L \longrightarrow G^L$ such that $\tau_x(y) = xy$. The map $p \longrightarrow p \circ \tau_x$ $P(G^L) \longrightarrow P(G^L)$ is an algebra automorphism and hence we see easily that $\rho^L \circ \tau_x$ is still a rational map from $G^L$ to $E(U^L)$. It is easy to see that $(G^L)_{\rho^L \circ \tau_x} = x^{-1}R$.

Now suppose $x$ is in $R$. Then there exists one and only one rational map: $G^L \dashrightarrow E(U^L)$ whose domain contains $R$ and whose value at every $y$ in $R$ is $\rho^L(x)\rho^L(y)$. (If $\rho^L = \sum f_i \otimes e_i$ with the $e_i$ linearly independent in $E(U^L)$, then $\sum f_i \otimes \rho^L(x)e_i$ has those properties and is unique because of the denseness of $R$.) Denote this rational map by $\rho^L(x)\rho^L$. If $x$ and $y$ are in $G$, we have $(\rho^L \circ \tau_x)(y) = \rho^L(xy) = \rho(xy) = \rho(x)\rho(y) = \rho^L(x)\rho^L(y) = (\rho^L(x)\rho^L)(y)$. Thus for $x$ in $G$, these rational maps $\rho^L \circ \tau_x$ and $\rho^L(x)\rho^L$ coincide on $G$. Now $G$ is a unicity set in $G^L$ and hence, by Lemma 6,

$\rho^L \circ \tau_x = \rho^L(x)\rho^L$ for every x in $G^L$. But $(G^L)_{\rho^L(x)\rho^L} \supset R$ and hence $(G^L)_{\rho^L \circ \tau_x} \supset R$. Thus $x^{-1}R \supset R$ and therefore $R \supset GR$.

Furthermore, $\rho^L(xy) = \rho^L(x)\,\rho^L(y)$ whenever x is in G and $y$ is in R.

Let $\sigma_y(x) = xy)$ and form $\rho^L \circ \sigma_y$ and $\rho^L\rho^L(y)$. For y in R, it follows as before that $\rho^L \circ \sigma_y = \rho^L\rho^L(y)$, $(G^L)_{\rho^L\rho^L(y)} \supset R$ and $(G^L)_{\rho^L \circ \sigma_y} = Ry^{-1}$. Hence $Ry^{-1} \supset R$ and therefore $R \supset RR$. By Prop.2, $RR = G^L$. Hence $R = G^L$.

Thus $\rho^L$, $\rho^L \circ \sigma_y$ and $\rho^L\rho^L(y)$ are rational maps defined at every point of $G^L$ for every y in $G^L$ and further, $\rho^L \circ \sigma_y = \rho^L\rho^L(y)$. Hence $\rho^L(xy) = \rho^L(x)\,\rho^L(y)$ for all x, y in $G^L$ so $\rho^L$ is a homomorphism.

In particular, $\rho^L(x)\rho^L(x^{-1}) = \rho^L(I) = \rho(I) = I$. Thus $\rho^L(x)$ is an automorphism of $U^L$. Therefore $\rho^L$ is a rational representation of $G^L$ by automorphisms of $U^L$. Since G is a unicity set in $G^L$, there can be only one such rational map coinciding with $\rho$ on G.

Let $H^*$ be the algebraic hull of $\rho^L(G^L)$. Then $H^* \cap E(U)$ is an algebraic group and $H^* \cap E(U) \supset \rho(G)$. Hence $H^* \cap E(U) \supset H$ whence $H^L \subset (H^* \cap E(U))^L \subset H^*$. Now let p be in $P(E(U^L))$ and suppose p is zero on $H^L$. Then $p \circ \rho^L$ is a rational function on $G^L$ which is zero on G. But G is a unicity set in $G^L$ and therefore $p \circ \rho^L$ is zero on $G^L$, i.e., p is zero on $\rho^L(G^L)$ and so on $H^*$. Therefore $H^* \subset H^L$ and so $H^* = H^L$. Q.E.D.

## 6. Specializations, Generic Points and Dimension.

Let $U$ be a K-space, $L$ a field containing $K$. As before, we identify $P(U)$ with its canonical image in $P(U^L)$. For $s$ in $U^L$, the elements $p(x)$, with $p$ in $P(U)$, constitute a ring which we denote by $K[s]$. Clearly $K \subset K[s] \subset L$. $K[s]$ is generated, as a K-algebra, by the elements $\lambda(s)$ with $\lambda \in U^*$. We denote the field of quotients of $K[s]$ by $K(s)$.

Let $L'$ be another field containing $K$.

Def. An element $s'$ in $U^{L'}$ is called a specialization of $s$ (in $U^L$) relative to $K$ if for every $p$ in $P(U)$, $p(s) = 0$ implies $p(s') = 0$. We denote such a specialization by $s \dashrightarrow s'$. This means that there exists a K-algebra epimorphism: $K[s] \dashrightarrow K[s']$ mapping each $p(s)$ onto $p(s')$.

Def. $s'$ is called a generic specialization of $s$ if $s$ is also a specialization of $s'$, i.e., if the epimorphism: $K[s] \dashrightarrow K[s']$ is also a monomorphism. If $s'$ is a specialization of $s$, the subring of $K(s)$ consisting of all fractions $\frac{p(s)}{q(s)}$ with $p$, $q$ in $P(U)$ and $p(s') \neq 0$ is called the specialization ring of the specialization $s \dashrightarrow s'$.

There is one and only one extension of the epimorphism $K[s] \dashrightarrow K[s']$ to an epimorphism of the specialization ring of $s \dashrightarrow s'$ onto $K(s')$. $s'$ is a generic specialization of $s$ if and only if the specialization ring of $s \dashrightarrow s'$ is $K(s)$ and the map $K(s) \dashrightarrow K(s')$ is an isomorphism.

If $G$ is an algebraic group of automorphisms of a $K$-space $U$, the elements of $G^L$ are called generalized points of $G$. If every point of $G$ is a specialization of the generalized point $s$ in $G^L$, we say that $s$ is a generic point of $G$.

Let $G$ be an algebraic group with associated ideal $\mathcal{A}$. Suppose $G$ has a generic point $s$. Then $p$ is in $\mathcal{A}$ if and only if $p(s) = 0$. Hence $\mathcal{A}$ is a prime ideal, i.e., $G$ is irreducible.

Now suppose that $G$ is irreducible. Then the ring $R(G)$ of rational functions on $G$ is a field $L$. In fact, since the ideal associated with $G$ is a prime ideal, $P(G)$ is an integral domain. Let $s$ be the element of $E(U^L)$ which is determined by the condition that $\lambda(s)$ is the restriction to $G$ of $\lambda$ for every $\lambda$ in $E(U)^*$. Then $p(s)$ is the restriction of $p$ to $G$ for every $p$ in $P(E(U))$. Therefore $p(s) = 0$ if and only if $p$ is zero on $G$. Thus every point of $G$ is a specialization of $s$ relative to $K$ and $s$ is a zero of the ideal $\mathcal{A}$ associated with $G$.

The ideal associated with $G^L$ is $\mathcal{A}^L$ and $s$ is also a zero of $\mathcal{A}^L$. Let $d$ be the determinant function on $E(U^L)$. Then $d(s)$ is the restriction of $d$ to $G$. Hence $d(s) \neq 0$. Hence $s$ is an automorphism. It follows that $s$ is in $G^L$ and thus $s$ is a generic point of $G$.

Theorem 13. Let $G$ be an irreducible algebraic group and $s$ a generic point of $G$. Then every generalized point $s'$ of $G$ is a specialization of $s$ and $s'$ is a generic point of $G$ if and only if $s'$ is a generic specialization of $s$. If $L$ is a field containing $K$ and if $t$ is an automorphism of $U^L$ such that $t$ is a specialization of $s'$ relative to $K$, then $t$ is in $G^L$.

Proof: Supose $s'$ is an element of $G^{L'}$. If $\mathcal{O}$ is the ideal associated with $G$, then, by Theorem 11, $\mathcal{O}^{L'}$ is the ideal associated with $G^{L'}$. If $p$ is any element of $P(E(U))$ such that $p(s) = 0$ then $p$ is in $\mathcal{O}$ since $s$ is generic. Hence $p$ is in $\mathcal{O}^{L'}$, whence $p(s') = 0$. Therefore $s'$ is a specialization of $s$.

Suppose $s'$ is a generic point of $G$. Then $q(s') = 0$ if and only if $q(s) = 0$, whence the specialization ring of $s \longrightarrow s'$ is $K(s)$. Further it is now clear that the epimorphism: $K(s) \longrightarrow K(s')$ is an isomorphism. Hence $s'$ is a generic specialization of $s$. On the other hand, if $s'$ is a generic specialization of $s$ then clearly, $s$ is a specialization of $s'$. Since $s' \longrightarrow s$ and $s \longrightarrow t$ implies $s' \longrightarrow t$, every point of $G$ is a specialization of $s'$. Therefore $s'$ is a generic point of $G$.

Now let $L \supset K$ and $t$ an automorphism of $U^L$ such that $s' \longrightarrow t$. Then $\mathcal{O}(s') = 0$ and hence $\mathcal{O}(t) = 0$. But then $\mathcal{O}^L(t) = 0$. Thus, by Theorem 11, $t$ is in $G^L$. Q.E.D.

Def. If $G$ is an irreducible algebraic group, the dimension of $G$ is defined as the transcendence degree $\{R(G): K\}$ of $R(G)$ over $K$. If $G$ is an arbitrary algebraic group, the dimension of $G$ is defined to be the dimension of its component of the identity $G_1$.

If $s$ is in $U^L$, we define $\dim_K(s) = \{K(s): K\}$.

Theorem 14. If $s$ is in $U^L$ and $s \longrightarrow s'$ relative to $K$, then $\dim_K(s') \leq \dim_K(s)$ and equality holds if and only if $s'$ is a generic specialization of $s$.

Proof: If $s \longrightarrow s'$, we have a $K$-algebra epimorphism of $K[s]$ onto $K[s']$. Hence the transcendence degree of $K(s) \geq$ transcendence degree of $K(s')$.

If $s'$ is a generic specialization of $s$, $K(s) \approx K(s')$, hence $\dim_K(s) = \dim_K(s')$.

Suppose $\dim_K(s) = \dim_K(s')$ p d and choose a transcendence basis $v_1, \ldots, v_d$ of $K(s')$ over $K$ such that $v_1, \ldots, v_d$ are in $K[s']$. Choose $w_i$ in $K[s]$ such that $\phi(w_i) = v_i$ where $\phi$ is the specialization homomorphism: $K[s] \longrightarrow K[s']$. Then $w_1, \ldots, w_d$ is a transcendence basis for $K(s)$ over $K$ whence $K(s)$ is algebraic over $K(w_1, \ldots, w_d)$. Let $R$ be the specialization ring in $K(s)$ of our specialization $s \longrightarrow s'$ and extend $\phi$ to a homomorphism $\phi$: $R \longrightarrow K(s')$. Clearly $K(w_1, \ldots, w_d) \subset R$.

The restriction of $\phi$ to $K(w_1, \ldots, w_d)$ is a monomorphism. If $f$ is any polynomial with coefficients in $K[w_1, \ldots, w_d]$, let $f^\phi$ denote the polynomial obtained by applying $\phi$ to the coefficients of $f$. Take $x \neq 0$ in $K[s]$ and let $f$ be the minimum polynomial of $x$ over $K[w_1, \ldots, w_d]$. Since $x \neq 0$, $f(0) \neq 0$ and hence $f^\phi(0) \neq 0$. Therefore $\phi(x) \neq 0$. Thus $\phi$: $K[s] \longrightarrow K[s']$ is a monomorphism and hence also an isomorphism, i.e., $s'$ is a generic specialization of $s$.

Theorem 15. Let $G$ be an algebraic group of automorphisms of the $K$-space $U$, $s$ a generalized point of $G$. Then $\dim_K(s) \leq \dim_K(G)$. If $G$ is irreducible, then equality holds if and only if $s$ is a generic point of $G$.

Proof: Let $G_1$ be the component of the identity of $G$ and let $e_1, \ldots, e_n$ be elements of $G$ such that $G = \bigcup_{i=1}^{n} e_i G_1$. Then for every $L \supset K$, $G^L = \bigcup_{i=1}^{h} e_i (G_1)^L$ and $(G_1)^L$ is the component of the identity of $G^L$. Thus every generalized point $s$ has the form $s = e_i s_1$ with $s_1$ a generalized point of $G_1$. Since the map $p \longrightarrow p \cdot e_i$

is a K-automorphism of $P(U)$, it follows that $K(s) = K(s_1)$. Hence $\dim_K(s) = \dim_K(s_1)$. Let $t$ be a generic point of $G_1$ such that $p(t)$ is the restriction of $p$ to $G_1$ for every $p$ in $P(E(V))$. Then $K(t) = R(G_1)$. Hence $\dim_K(t) = \dim_K(G_1) = \dim_K(G)$. Since $t$ is generic $t \dashrightarrow s_1$ and therefore $\dim_K(s) = \dim_K(s_1) \leq \dim_K(t) = \dim_K(G)$.

Now suppose $G$ is irreducible. Then $\dim_K(s) = \dim_K(t)$ if and only if $s$ is a generic specialization of $t$. Thus $\dim_K(s) = \dim_K(G)$ if and only if $s$ is a generic point of $G$.

Theorem 16. Let $G$ be an algebraic group and $H$ an algebraic subgroup of $G$. Then $\dim_K(H) \leq \dim_K(G)$ and equality holds if and only if $H$ is of finite index in $G$.

Proof: Let $G_1$ and $H_1$ be the components of the identity in $G$ and $H$ respectively. $H \cap G$ is an algebraic group of finite index in $H$ and hence $H \cap G_1 \supset H_1$. A generic point of $H_1$ is a generalized point of $G_1$ and therefore $\dim(H) \leq \dim(G)$.

If equality holds then a generic point of $H_1$ is also a generic point of $G_1$. Therefore $H_1 = G_1$ so that $H \supset G_1$ and thus is of finite index in $G$.

Conversely, if $H$ is of finite index in $G$, then $H_1$ is of finite index in $G$. Therefore $H_1 = G_1$ and thus, $\dim(H) = \dim(G)$.

Theorem 17. If $L$ is an extension field of $K$ and $G$ is an algebraic group of automorphisms of a finite-dimensional $K$-space, then $\dim_L(G^L) = \dim_K(G)$.

Proof: We know that $(G_1)^L = (G^L)$, so that we may assume $G = G_1$. Now $R(G^L)$ is generated as a field by $R(G) \otimes L$. Hence a transcendency basis for $R(G)$ over $K$ is also a transcendency basis for $R(G^L)$ over $L$. Hence the result.

## 7. Applications to Lie Algebras.

Recall that if $G$ is an algebraic group with associated ideal $\mathcal{O}$ then $G^\circ = \{e \text{ in } E \mid D_e(\mathcal{O}) \subset \mathcal{O}\}$. $D'_e$ was defined so that $D'_e(p) = D_e(p)(I)$. $x$ is in $G^\circ$ if and only if $D'_x$ annihilates $\mathcal{O}$.

Prop. 3. Let $G_1$ be the component of the identity in $G$. Then $G_1^\circ = G^\circ$

Proof: Clearly $G_1^\circ \subset G^\circ$. On the other hand, let $p$ be a polynomial function on $E(U)$ such that $p$ is zero on $G_1$. Then, by Theorem 6, there exists $p_1$ in $P(E(U))$ such that $pp_1$ is zero on $G$ and $p_1(I) \neq 0$. Now take $e$ in $G^\circ$. Then $0 = D'_e(pp_1) = D'_e(p)p_1(I) + p(I)D'_e(p_1)$. Therefore $D'_e(p)p_1(I) = 0$, whence $D'_e(p) = 0$. Hence $e$ is in $G_1^\circ$ and so $G^\circ \subset G_1^\circ$. Thus $G_1^\circ = G^\circ$. Q.E.D.

Theorem 18. Let $L$ be any extension field of $K$. Then $(G^L)^\circ = (G^\circ)^L$.

Proof: Let $\mathcal{O}$ be the ideal associated with $G$. Then $\mathcal{O}^L$ is the ideal associated with $G^L$ and hence it is clear that $(G^\circ)^L \subset (G^L)^\circ$.

Now take $e$ in $(G^L)^\circ$ and let $(l_i)$ be a basis for $L$ over $K$. Write $e = \sum l_i e_i$ with $e_i \in E(V)$. Then $D_e = \sum l_i D_{e_i}$. Then, for $p$ in $\mathcal{O}$, $D_e(p) = \sum l_i D_{e_i}(p)$. On the other hand, $D_e(p)$ is in $\mathcal{O}^L$ so that we may write $D_e(p) = \sum l_i p_i$ with $p_i$ in $\mathcal{O}$. Therefore $D_{e_i}(p) = p_i$ is in $\mathcal{O}$ whence the $e_i$ are in $G^\circ$. Thus $e$ is in $(G^\circ)^L$ whence $(G^L)^\circ \subset (G^\circ)^L$. Q.E.D.

Let $L$ be an extension field of $K$ and let $\delta$ be a $K$-derivation of $L$. If $A$ is any $K$-algebra then $\delta$ induces a derivation of $A^L = A \otimes_K L$ (still denoted by $\delta$) such that $\delta(a \otimes l) = a \otimes \delta l$. For every $\lambda$ in $A^* \subset (A^L)^*$ and $u$ in $A \otimes L$ we have

$$\lambda(\delta(u)) = \delta(\lambda(u)) .$$

From now on we shall always use the same letter for a derivation of a field $L$ and for the corresponding derivation of $A^L$ where $A$ is any algebra over $K$.

Theorem 19. Let $G$ be an algebraic group of automorphisms of the $K$-space $U$ and let $L$ be an extension field of $K$. Let $\delta$ be any $K$-derivation of $L$. If $s$ is any element of $G^L$, then $s^{-1}\delta(s)$ is in $(G^\circ)^L$. Furthermore, if $G$ is irreducible and if $s$ is a generic point of $G$, then, for every $x$ in $(G^\circ)^L$, there exists one and only one $K$-derivation $\delta_x$ of $K(s)$ such that $\delta_x(s) = sx$ (where $\delta_x$ is used also to denote the derivation of $E^{K(s)}$ obtained canonically from the derivation $\delta_x$ of $K(s)$). The map $x \longrightarrow \delta_x$ is a $K(s)$-linear isomorphism of $(G^\circ)^{K(s)}$ onto the $K(s)$-space of all $K$-derivations of $K(s)$.

Proof: Write $E = E(U)$ and take $\lambda$ in $E^*$. Then $D_{s^{-1}\delta(s)}(\delta)\{s\} = \lambda(ss^{-1}\delta(s)) = \lambda(\delta(s)) = \delta(\lambda(s))$. Consider the maps $p \longrightarrow D_{s^{-1}\delta(s)}(p)\{s\}$ and $p \longrightarrow \delta(p(s))$. These are differentiations, at $s$, of $P$ into $K(s)$ which are zero on constants and which agree on $E^*$. Hence they agree on all of $P$. Thus

$$D_{s^{-1}\delta(s)}(p)\{s\} = \delta(p(s)).$$

Suppose $p$ is zero on $G$. Then $p(s) = 0$ so that $D_{s^{-1}\delta(s)}(p)\{s\} = \delta(p(s)) = 0$, i.e., $(D_{s^{-1}\delta(s)}(p).s)\{I\} = 0$,

i.e., $D_{s^{-1}\delta(s)}(p.s)\{I\} = 0$.

Let $\mathcal{O}$ be the ideal associated with $G$. Then $\mathcal{O}^L$ is the ideal associated with $G^L$. Since $s$ is in $G^L$, we have $\mathcal{O}^L = \mathcal{O}^L.s = (\mathcal{O} \otimes L).s = (\mathcal{O} \cdot s)^L$. Hence, by $L$-linearity, the above gives

$D_{s^{-1}\delta(s)}(q) = 0$ for all $q$ in $\mathcal{O}^L$. Therefore $s^{-1}\delta(s)$ is in $(G^L)^\bullet = (G^\bullet)^L$.

Now suppose that $G$ is irreducible and that $s$ is a generic point of $G$. For $e$ in $G^\circ$, $D_e$ induces a derivation $\delta_e$ of $P(G)$. Since the map $p \longrightarrow p(s)$ is an isomorphism of $P(G)$ onto $K[s]$, we may define a derivation $\delta_e$ of $K[s]$ such that $\delta_e(p(s)) = d_e(p)\{s\}$. This $\delta_e$ extends uniquely to a derivation (still denoted by $\delta_e$) of $K(s)$. This gives a $K$-linear map $e \longrightarrow \delta_e$ of $G^\circ$ into the derivation algebra of $K(s)$ over $K$. The map $e \longrightarrow \delta_e$ clearly extends to a $K(s)$-linear map of $(G^\bullet)^{K(s)}$ into the derivation algebra of $K(s)$.

If $\lambda$ is $E^*$ and $e$ is in $G^\bullet$, we have $D_e(\lambda)\{s\} = \lambda(se)$ so that $\delta_e(\lambda(s)) = \lambda(se)$. By linearity, this gives that $\delta_s(\lambda(s)) = \lambda(sx)$ for all $x$ in $(G^\bullet)^{K(s)}$. But $\lambda$ commutes with $\delta_x$, i.e., $\lambda(\delta_x(s)) = \lambda(sx)$ for all $x$ in $(G^\bullet)^{K(s)}$. Hence $\delta_s(s) = \lambda(sx)$.

Conversely, if $\delta$ is any $K$-derivation of $K(s)$ and $\delta(s) = sx$ then $\delta(\lambda(s)) = \lambda(sx)$ for every $\lambda$ in $E^*$ whence $\delta = \delta_x$. This completes the proof.

Theorem 20. Let $G$ be an algebraic group. Then $\dim_K(G) = [G^\circ : K]$ (the dimension of $G^\circ$ as a $K$-space).

Proof: We may assume that $G$ is irreducible. Now $[G^\circ : K] = [(G^\bullet)^{R(G)} : R(G)]$ and, by Theorem 19, there exists an $R(G)$-linear isomorphism $x \longrightarrow \delta_x$ of $(G^\circ)^{R(G)}$ onto the $R(G)$-space of all $K$-derivations of $R(G)$. Hence it suffices to show that the dimension of the $R(G)$-space of all $K$-derivations of $R(G)$ equals the transcendency degree of $R(G)$ over $K$.

In order to do this we show first that if $\ell_1, \ldots, \ell_n$ are K-linearly independent elements of R(G), then $\ell_1^p, \ldots, \ell_n^p$ are K-linearly independent where p = 1 if the characteristic of K is zero and p = characteristic of K otherwise. Let $\bar{K}$ be the algebraic closure of K. $G^{\bar{K}}$ is irreducible and so $R(G^{\bar{K}})$ is a field. We have an isomorphic imbedding $R(G) \otimes \bar{K} \longrightarrow R(G^{\bar{K}})$. Now suppose we have elements $k_i$ in K, not all 0, such that $\sum k_i \ell_i^p = 0$. Choose $c_i$ in $\bar{K}$ such that $c_i^p = k_i$. Then $\sum \ell_i^p \otimes c_i^p = \sum (\ell_i \otimes c_i)^p = 0$ and thus $\sum \ell_i \otimes c_i = 0$ since fields have no nilpotent elements. If the $\ell_i$ are linearly independent over K, then each $c_i = 0$ whence each $k_i = 0$.

Now write L for R(G) and let m be the dimension of the L-space of all K-derivations of L. m is finite because L is finitely

generated over K. We can find a basis $D_1, \ldots, D_m$ for the space of derivations and elements $u_1, \ldots, u_m$ in L such that $D_i(u_j) = \delta_{ij}$. Put $F = K(u_1, \ldots, u_m)$. Then every derivation of L that annihilates F must be 0. We claim that L is a separable algebraic extension of F. We have $L = F(v_1, \ldots, v_n)$. Let k be the smallest index such that L is separable algebraic over $F(v_1, \ldots, v_k)$. If $k > 0$ there are two cases: (1) $v_k$ is transcendental over $F(v_1, \ldots, v_k)$ that annihilates F. (2) $v_k$ is algebraic and inseparable over $F(v_1, \ldots, v_{k-1})$. Then $p \neq 1$, i.e., the characteristic of K is $p \neq 0$ and $v_k$ is not in $F(v_1, \ldots, v_{k-1})[v_k^p]$. Then we can find a derivation D of $F(v_1, \ldots, v_k)$ such that D annihilates $F(v_1, \ldots, v_{k-1})[v_k^p]$ and $D(v_k) = 1$.

Thus, in either case, there exists a non-zero derivation of $F(v_1, \ldots, v_k)$ that annihilates F. Since L is separably algebraic over $F(v_1, \ldots, v_k)$, this derivation can be extended to a derivation of L. This is a contradiction and thus we conclude that L is separably algebraic over F.

Now we shall show that $u_1, \ldots, u_m$ are algebraically independent over K. Suppose this is false and let f be a non-zero polynomial of least possible total degree such that $f(u_1, \ldots, u_m) = 0$. Then $D_i(f(u_1, \ldots, u_m)) = 0$, i.e., $f_i(u_1, \ldots, u_m) = 0$ where $f_i$ is the derivative of f with respect to the $i^{th}$ variable. By the minimality of f, this implies that $f_i = 0$ for each i. Hence $p \neq 1$ and $f(w_1, \ldots, w_m) = g(w_1^p, \ldots, w_m^p)$ where the $w_i$ are variables, i.e., $f(w_1, \ldots, w_m) = \sum_j k_j z_j^p$ where $k_j$ is in K, $k_j \neq 0$, and the $z_j$ are monomials in $w_1, \ldots, w_m$. Let $y_j$ be the monomial in $u_1, \ldots, u_m$

obtained by replacing each $w_i$ with $u_i$ in $z_j$. Then $\sum_j k_j y_j^p = 0$. By what we have shown above, this implies that the $y_j$ are linearly dependent over $K$ so that there exist elements $k_j'$ in $K$, not all $0$, such that $\sum_j k_j' y_j = 0$. Then $\sum_j k_j' z_j$ is a non-zero polynomial vanishing at $(u_1, \ldots, u_m)$. This contradicts the minimality of $f$ and hence the elements $u_1, \ldots, u_m$ are algebraically independent over $K$. Thus the transcendence degree of $L$ over $K$ = $m$ = dimension of the space of $K$-derivations of $L$. This completes the proof of Theorem 20.

Corollary. Let $G$ be an algebraic group and $H$ an algebraic subgroup of $G$. Then $H$ is of finite index in $G$ if and only if $G^\circ = H^\circ$.

Proof: We know that $H^\circ \subset G^\circ$. By Theorem 20, $H^\circ = G^\circ$ if and only if $\dim(H) = \dim(G)$. By Theorem 16, this last holds if and only if $H$ is of finite index in $G$. Q.E.D.

Theorem 21. If $A$ is an irreducible algebraic group of automorphisms of the $K$-space $V$ and if $K$ has characteristic $0$ then $A = G_{A^\circ}$.

Proof: By the definition of $G_{A^\circ}$, $G_{A^\circ} \subset A$. By the above Corollary, $G_{A^\circ}$ has finite index in $A$. Since $A$ is irreducible, $G_{A^\circ} = A$.

Theorem 22. Let $G$ be an algebraic group of automorphisms of the $K$-space $V$. Then $G^\circ$ is contained in the associative algebra $\{G\}$ generated by the elements of $G$.

Proof: For any extension field $L$ of $K$, $\{G^L\} = \{G\}^L$. In fact it is clear that $\{G\}^L \subset \{G^L\}$. Take $\lambda$ in $E(V)^*$ and suppose $\lambda(G) = (0)$. Then $\lambda(G^L) = (0)$ so that $\lambda(\{G^L\}) = 0$. Therefore $\{G^L\} = \{G\}^L$.

Let $s$ be a generic point of $G$, and put $L = K(s)$. Take $x$ in $G^\bullet$. Then there exists a $K$-derivation $\delta_x$ of $L$ such that $\delta_x(s) = sx$. Since $s$ is in $\{G^L\} = \{G\}^L$, $s = \sum \ell_i s_i$ with $\ell_i$ in $L$ and $s_i$ in $\{G\}$. Then $\delta_x(s) = \sum \delta_x(\ell_i)s_i$ is in $\{G\}^L$. Therefore $sx$ is in $\{G\}^L$. Hence $x$ is in $G^L\{G^L\} = \{G\}^L$. Hence $G^\bullet \subset \{G\}^L \cap E(V) = \{G\}$. Q.E.D.

## 8. Differentials of Rational Representations.

Let $G$ be an irreducible algebraic group of automorphisms of the finite-dimensional $K$-space $V$ and let $\rho$ be a rational representation of $G$ by automorphisms of another finite-dimensional $K$-space $U$. Let $T$ be the subring of $R(G)$ consisting of all $\frac{p}{q}$ with $p$, $q$ in $P(G)$ and $q(1) \neq 0$.

For $x$ in $G^*$, let $d_x$ denote the corresponding derivation of $R(G)$ (induced by $D_x$). If $\frac{p}{q}$ is in $T$, then $d_x(\frac{p}{q}) = \frac{1}{q^2}(qd_x(p)-pd_x(q))$ is in $T$. Thus $d_x(T) \subset T$. Define $d'_x(p) = d_x(p)\{I\}$. $d'_x$ is a differentiation at $I$, of $T$ into $K$.

Let $\mu$ be any element of $E(U)^*$. Then $\mu \circ \rho$ is in $T$. Consider the map $\mu \longrightarrow d'_x(\mu \circ \rho)$. This is a linear function on $E(U)^*$ and hence (since $E \cong E^{**}$) there exists one and only one element, denoted by $\rho^*(x)$, in $E(U)$ such that for every linear function $\mu$, $\mu(\rho^*(x)) = d'_x(\mu \circ \rho)$. The map $\rho^* : G^* \longrightarrow E(U)$ is linear and is called the differential of $\rho$.

Let $x$ be in $G^*$, $s$ in $G$, $\mu$ in $E(U)^*$. Then

$$\begin{aligned} d_x(\mu \circ \rho)\{s\} &= (d_x(\mu \circ \rho).s)(I) \\ &= d_x((\mu \circ \rho).s)(I) \quad \text{since } d_x \text{ commutes with right translations} \\ &= d_x(\mu.\rho(s) \circ \rho)(I) = d'_x(\mu.\rho(s) \circ \rho) \\ &= (\mu.\rho(s))\{\rho^*(x) \quad = \mu(\rho(s)\rho^*(x)) \\ &= D_{\rho^*(x)}(\mu)\{\rho(s)\} \\ &= (D_{\rho^*(x)}(\mu) \circ \rho)\{s\} \ . \end{aligned}$$

Therefore $d_x(\mu \circ \rho) = D_{\rho^*(x)}(\mu) \circ \rho$. This extends immediately by formal properties to give

$$d_x(q \circ \rho) = D_{\rho^*(x)}(q) \circ \rho$$

for every $q$ in $P(E(U))$.

Now we show that $\rho^*$ is a Lie algebra homomorphism of $G^*$ into $E(U)$. Take $x$, $y$ in $G^*$. Then from our definitions, $[d_x,d_y] = d_{[x,y]}$ and

$d'_{[x,y]} = (d_x \circ d_y - d_y \circ d_x)' = d'_x \circ d_y - d'_y \circ d_x$ . Take $\mu$ in $E(U)^*$ .

Then $\mu([\rho^\circ(x), \rho^\circ(y)]) = \mu(\rho^\circ(x)\rho^\circ(y) - \rho^\circ(y)\rho^\circ(x)) =$

$= D_{\rho^\circ(y)}(\mu)(\rho^\circ(x)) - D_{\rho^\circ(x)}(\mu)(\rho^\circ(y))$

$= d'_x(D_{\rho^\circ(y)}(\mu) \circ \rho) - d'_y(D_{\rho^\circ(x)}(\mu) \circ \rho)$

$= d'_x(d_y(\mu \circ \rho)) - d'_y(d_x(\mu \circ \rho)$

$= d'_{[x,y]}(\mu \circ \rho)$

$= \mu(\rho^\circ[x,y])$ .

Hence $[\rho^\circ(x), \rho^\circ(y)] = \rho^\circ[x,y]$ .

Theorem 23. Let G be an irreducible algebraic group of automorphisms of the finite dimensional K-space V and let $\rho$ be a rational representation of G by automorphisms of another finite-dimensional K-space U. Let H be the algebraic hull of $\rho(G)$. Then H is irreducible.

Proof: If q is in P(H) then $q \circ \rho$ is in T. Now let $\mathcal{L}$ be the ideal associated with H. Then q is in $\mathcal{L}$ if and only if $q \circ \rho = 0$ . Therefore $\mathcal{L}$ is a prime ideal since T has no zero-divisor. Therefore H is irreducible. Q.E.D.

Now we assert that $\rho^\circ(G^\circ) \subset H^\circ$ . We know that $D_{\rho^\circ(x)}(q) \circ \rho = d_x(q \circ \rho)$ for all q in P(H). If q is in $\mathcal{L}$ then $q \circ \rho = 0$ . Therefore $D_{\rho^\circ(x)}(q) \circ \rho = 0$ whence $D_{\rho^\circ(x)}(q)$ is in $\mathcal{L}$ . Thus $D_{\rho^\circ(x)}(\mathcal{L}) \subset \mathcal{L}$ which proves the assertion.

Theorem 24. Let $\rho$ be a rational representation of the irreducible algebraic group G of automorphisms of a K-space V be automorphisms of a K-space U. Then $\rho$ induces a Lie algebra homomorphism $\rho^\circ$ of $G^\circ$ into the Lie algebra $H^\circ$ of the algebraic group hull H of $\rho(G)$ . For every x in $G^\circ$ and every q in P(E(U)), $d_x(q \circ \rho) = D_{\rho^\circ(x)}(q) \circ \rho$.

If L is any field containing K then $(\rho^L)^\cdot = (\rho^\cdot)^L$. If R(G) is separably generated over the subfield $R(H) \circ \rho$ then $\rho^\cdot(G) = H^\cdot$.

Proof: There remains only to verify the last two statements. Take $\mu$ in $E(U)^*$. Then the element $\mu \circ \rho^L$ of $R(G^L)$ is canonical extension of the element $\mu \circ \rho$ of R(G). Therefore if x is in $G^\cdot$, $d_x(\mu \circ \rho^L)$ coincides with $d_x(\mu \circ \rho)$ on G. Hence $d'_x(\mu \circ \rho^L) = d_x(\mu \circ \rho^L)(I) = d_x(\mu \circ \rho)(I) = d'_x(\mu \circ \rho)$. Then, by definition of $\rho^\cdot$ and $(\rho^L)^\cdot$, $\mu((\rho^L)^\cdot(x)) = \mu(\rho^\cdot(x))$. Therefore $(\rho^L)^\cdot(x) = \rho^\cdot(x)$ for x in $G^\cdot$. Hence $(\rho^L)^\cdot = (\rho^\cdot)^L$.

Take z in $H^\cdot$ and consider the derivation $d_z$ of R(H). This carries over to a K-derivation of $R(H) \circ \rho \subset R(G)$. Since R(G) is separably generated over $R(H) \circ \rho$, this derivation extends to a derivation $\delta$ of R(G). Thus there exists a K-derivation $\delta$ of R(G) such that $\delta(f \circ \rho) = d_z(f) \circ \rho$ for every f in R(H). Let s be the generic point of G such that $p(s) = p|_G$ for every p in P(E(V)) where $p|_G$ is the restriction of p to G. Then, for every f in R(H), $f(\rho^{R(H)}(s)) = f \circ \rho$ [first for f in P(H) and then this extends to all f in R(H)]. Extend $\delta$, as usual, to a derivation (still denoted by $\delta$) of $E(U)^{R(G)}$ and take $\mu$ in $E(U)^*$. Then

$$\mu(\delta(\rho^{R(G)}(s))) = \delta(\mu(\rho^{R(G)}(s))) = \delta(\mu \circ \rho) = d_z(\mu|_H) \circ \rho$$
$$= d_z(\mu|_H)(\rho^{R(G)}(s)) = \mu(\rho^{R(G)}(s)z) .$$

Therefore

(*) $$\underline{\delta(\rho^{R(G)}(s)) = \rho^{R(G)}(s)z} .$$

On the other hand, put $t = s^{-1}\delta(s)$. By Theorem 19, $t$ is in $(G^\bullet)^{R(G)} = G^\bullet \otimes_K R(G)$. By the first part of our theorem, applied to $\rho^{R(G)}$, $d_t(\mu \circ \rho^{R(G)}) = D_{(\rho^{R(G)})^\bullet(t)}(\mu) \circ \rho^{R(G)}$. Hence

$$d_t(\mu \circ \rho^{R(G)})(s) = D_{(\rho^{R(G)})^\bullet(t)}(\mu)(\rho^{R(G)}(s)) = \mu(\rho^{R(G)}(s)(\rho^{R(G)})^\bullet(t))$$

From before, we know that

$$d_t(\mu \circ \rho^{R(G)})(s) = d_{s^{-1}\delta(s)}(\mu \circ \rho^{R(G)})(s) = \delta(\mu \circ \rho^{R(G)}(s))$$

$$= \mu(\delta(\rho^{R(G)}(s)) \quad .$$

Therefore $\rho^{R(G)}(s)(\rho^{R(G)})^\bullet(t) = \delta(\rho^{R(G)}(s))$. Hence, by (*), $\rho^{R(G)}(s)z = \rho^{R(G)}(s)(\rho^{R(G)})^\bullet(t)$ and so $(\rho^{R(G)})^\bullet(t) = z$, i.e., $(\rho^\bullet)^{R(G)}(t) = z$.

Now $t = \sum_{i=1}^{n} \ell_i x_i$ where $\ell_1, \ldots, \ell_n$ are K-linearly independent elements of $R(G)$, $\ell_1 = 1$ and the $x_i \in G^\circ$. Then $\sum \ell_i \rho^\circ(x_i) = z$ so that $\rho^\circ(x_1) = z$ and $\rho^\circ(x_i) = 0$ for $i > 1$. Therefore $z$ is in $\rho^\circ(G^\circ)$. Thus $\rho^\circ(G^\circ) = H^\circ$. Q.E.D.

Theorem 25. Let $G$ be an irreducible algebraic group of automorphisms of a K-space $V$ where $K$ has characteristic 0. Let $\rho$ be a rational representation of $G$ and let $t$ be an auxilliary variable. Then

$$\rho^{K\langle t\rangle} \exp(tx) = \operatorname{ext}(t\rho^\circ(x)) \quad .$$

Proof: Let $\delta$ be the derivation with respect to $t$ in the power series field $K\langle t\rangle$ and also write $\delta$ for the corresponding derivation of $E^{K\langle t\rangle}$. Then $\delta(\exp tx) = \exp(tx)x$. Now for $\lambda$ in $E(V)^*$, we have

$$\delta(\lambda(\exp(tx))) = \lambda\delta(\exp(tx)) = \lambda(\exp(tx)x) = D_x(\lambda)(\exp tx)$$

i.e., $\delta(\lambda(\exp(tx))) = D_x(\lambda)(\exp(tx))$. This extends immediately to give $\delta(f(\exp(tx))) = d_x(f)(\exp(tx))$ for every $f$ in $R(G)$ such that $f$ is defined at every point of $G^{K<t>}$. In particular, take $f = \mu \circ \rho$ with $\mu$ in $E(U)^*$ where $U$ is the K-space such that $\rho(G) \subset E(U)$. Then

$$\begin{aligned}\mu(\delta(\rho(\exp(tx)))) &= \delta((\mu \circ \rho)(\exp(tx))) \\ &= d_x(\mu \circ \rho)(\exp(tx)) \\ &= D_{\rho^\circ(x)}(\mu)(\rho(\exp(tx))) \\ &= \mu(\rho(\exp(tx)\,\rho^\circ(x)))\ .\end{aligned}$$

Therefore (*) $\quad \delta(\rho(\exp(tx))) = \rho(\exp(tx))\,\rho^\circ(x)$ .

This shows that $\rho(\exp(tx))$ is in $E(U)^{K\{\{t\}\}}$ where $K\{\{t\}\}$ is the ring of integral power series in $t$. Let $a$ be the "constant term" of $\rho(\exp(tx))$ in $E(U)$. Then the above differential equation (*) gives $\rho(\exp(tx)) = \exp(t\,\rho^\circ(x))a$. There exist $p$, $q$ in $P(G) \subset P(G^{K<t>})$ such that $q(I) \neq 0$ and $q(\lambda \circ \rho^{K<t>}) = p$. Hence

$$q(\exp(tx))\lambda(\rho(\exp(tx))) = p(\exp(tx))\ .$$

From this we see that $\lambda(a) = \lambda\rho(I)$ for all $\lambda$ in $E^*$. Hence $a = \rho(I)$. Thus $\rho(\exp(tx)) = \exp(t\,\rho^\circ(x))$. Q.E.D.

Theorem 26. Let $M$ be a representation space for a rational representation of an algebraic group $G$. Then every $G$-stable subspace of $M$ is also $G^\circ$-stable. If the base field has characteristic 0 and if $G$ is irreducible, then every $G^\circ$-stable subspace of $M$ is also $G$-stable.

Proof: Let $\rho$ be the given rational representation of $G$, and let $H$

be the algebraic group hull of $\rho(G)$. Since the group of all automorphisms of $M$ that maps a subspace $N$ into itself is an algebraic group, it follows that a subspace of $M$ is $\rho(G)$-stable if and only if it is H-stable. We know that $H^\circ$ is conatined in the associative algebra generated by the elements of $H$. Therefore every G-stable subspace of $M$ is also $H^\circ$-stable. Now $\rho^\circ(G^\circ) \subset H^\circ$ so the first part of the theorem is proved.

Now suppose that $G$ is irreducible and that the base field has characteristic 0. Let $N$ be a subspace of $M$ that is stable under $\rho^\circ(G^\circ)$. Let $K\langle t\rangle$ be the field of power series in the variable $t$. Then $\exp(t\rho^\circ(x))(N) \subset N^{K\langle t\rangle}$ for every $x$ in $G^\circ$. But, by Theorem 25, $\exp(t\rho^\circ(x)) = \rho\exp(tx)$ so that $\rho(\exp(tx))(N) \subset N^{K\langle t\rangle}$ for all $x$ in $G$.

Let $G_x$ be the smallest algebraic group whose Lie algebra contains $x$. From our discussion of $G_x$ (see the proof of Theorem 1), we know that $\exp(tx)$ is a generic point of $G_x$. It follows that $\rho(s)(N) \subset N$ for every $s$ in $G_x$. Thus $\rho(G_x)(N) \subset N$. But $G$ is the smallest algebraic group containing all of the $G_x$ with $x$ in $G^\circ$. Hence $\rho(G)(N) \subset N$. Q.E.D.

## 9. Characterization of the Differentials of Rational Representation.

Theorem 27. Let $G$ be an algebraic group of automorphisms of a K-space $V$. Let $\rho$ be a rational representation of $G$ and let $d$ be the determinant function on $G$. Then the representative functions associated with $\rho$ belong to $P[\frac{1}{d}]$, where $P$ is the algebra of all polynomial functions on $G$.

Proof: Let L be the algebraic closure of K and consider $G^L$ and $\rho^L$. This shows that without loss of generality, we may assume that K is algebraically closed. Let f be a representative function associated with $\rho$. If p and q are elements of P(E(V)), we denote by $\bar{p}$, $\bar{q}$ their restrictions to G. Let $\mathcal{O}$ be the ideal associated with G. We shall say that $\bar{q}$ is a denominator of f if $\bar{q}f = \bar{p}$. Let $\mathcal{L}$ denote the ideal generated by $\mathcal{O}$ and all of the denominators of f. Let D be the determinant function on E(V) so that $\bar{D} = d$. Since $G_f = G$, there exists, for every x in G, elements p, q in P(E(V)) such that $\bar{q}(x) \neq 0$ and $\bar{q}f = \bar{p}$. Thus it follows that while a zero of $\mathcal{L}$ is also a zero of $\mathcal{O}$, it is not a point of G. Hence every zero of $\mathcal{L}$ is a zero of D. Therefore it follows from the Hilbert Nullstellensatz that there exists a non-negative integer n such that $D^n$ is in $\mathcal{L}$. Thus

$$D^n = p_1q_1 + \dots p_kq_k + p$$

where p is in $\mathcal{O}$, the $q_i$ are denominators of f and $p_i$ are in P(E(V)). Take residue classes mod $\mathcal{O}$. Then we get $d^n = \bar{p}_1\bar{q}_1 + \dots + \bar{p}_k\bar{q}_k$ hence $d^nf = \bar{p}_1(\bar{q}_1f) + \dots + \bar{p}_k(\bar{q}_kf)$ is in P(G). Q.E.D.

Let d be the determinant function on E(V) and let $\sigma$ denote the trace function on E(V). Then for every e in E(V), $D_e(d) = \sigma(e)d$. To prove this note that for x in E(V), $D_e(d)(x) = (D_e(d).x)(I) = D_e(d.x)(I) = D_e(d(x)d)(I) = (D_e(d))(I)d(x)$. Thus $D_e(d) = (D_e(d)(I))d$. Write $d = f(\lambda_1,\dots,\lambda_p)$ where the $\lambda_i$ are in $E(V)^*$ and f is a polynomial. Then $D_e(d) = \sum_{i=I}^{p} f_i(\lambda_1, \dots, \lambda_p)D_e(\lambda_i)$ where $f_i$ is the derivative of f with respect to the $i^{th}$ variable.

$D_e(d)(I) = \sum_{i=1}^{p} f_i(\lambda_1(I), \ldots, \lambda_p(I))\lambda_i(e)$ . Now let $t$ be an auxilliary variable. $d(I + te) = 1 + t\sigma(e) + t^2(\ldots)$ . Hence the coefficient of $t$ in $f(\lambda_1(I) + t\lambda_1 e, \ldots, \lambda_p(I) + t\lambda_p(e))$ is $\sigma(e)$, i.e., $\sum_{i=1}^{p} f_i(\lambda_1(I), \ldots, \lambda_p(I))\lambda_i(e) = D_e(d)(I)$. Therefore $D_e(d)(I) = \sigma(e)$ so that $D_e(d) = \sigma(e)d$ .

Let $G$ be an algebraic group and let $R$ be the algebra of all representative functions on the universal enveloping algebra $U$ of $G^\circ$ . Consider the homomorphism: $P(E(V)) \longrightarrow R$ corresponding canonically to the identity representation of $G^\circ$ (see Section 2, p. 43) and denote this homomorphism by $p \longrightarrow p'$ . We know that this is a $G^\circ$-homomorphism, i.e., for every $x$ in $G^\circ$, $(D_x(p))' = x.p'$ and $p'(1) = p(I)$ . In particular, $d'(1) = 1$. Now let $x_1, \ldots, x_n$ be elements of $G^\circ$ . Then $d'(x_1 \ldots x_n) = ((x_1 \ldots x_n).d')(1) = (D_{x_1} \ldots D_{x_n}(d))'(1) =$

$= (D_{x_1} \ldots D_{x_n}(d))(I) = \sigma(x_1) \ldots \sigma(x_n)d(I) = \sigma(x_1) \ldots \sigma(x_n)$ .

$d'$ may also be obtained as follows: Consider the linear map: $G^\circ \longrightarrow K$ which sends each element of $G^\circ$ onto its trace. This map can be extended uniquely to a unitary algebra homomorphisms of $T(G^\circ)$ into $K$ where $T(G^\circ)$ is the tensor algebra built over $G^\circ$ . It is seen immediately that this map annihilates the ideal $J$ generated by all elements of the form $x \otimes y - y \otimes x - [x, y]$ with $x, y$ in $G^\circ$ and therefore, this map induces a unitary homomorphism of $U$ into $K$. This last map evidently coincides with the function $d'$ defined above. Similarly there exists a unitary algebra homomorphism: $T(G^\circ) \longrightarrow K$ sending each $x$ in $G^\circ$ onto $-\sigma(x)$ . This induces a homomorphism $z$ , of $U$ into $K$ such that $z(1) = 1$, $z(x_1 \ldots x_m) = (-1)^m \sigma(x_1) \ldots \sigma(x_m)$ . Now, recalling that

$d'z = d'\otimes z$ (diagonal map), we see that d'z is the constant 1. Now, for x in $G^\circ$, $x.z = -\sigma(x)z = z.x$. Thus the translates of z span a one-dimensional space and hence, z is a representative function on U.

Theorem 28. Let G be an irreducible group of automorphisms of the finite-dimensional K-space V. Let $G^\circ$ be the Lie algebra of G and let S be the subalgebra of R (the representative functions on $U(G^\circ)$) generated by the constants and the representative functions associated with the identity representation of $G^\circ$. Let $\phi$ be a representation of $G^\circ$. Then $\phi$ is the differential $\rho^\circ$ of a rational representation $\rho$ of G if and only if $R(\phi) \subset S[z]$ where $R(\phi)$ is the space of representative functions associated with $\phi$.

Proof: Assume first that $\phi = \rho^\circ$. Let $M_\phi$ be the representation space of $\phi$, put $E_\phi = E(M_\phi)$ and choose f in $E_\phi^*$. Consider the function $f \circ \rho$ in R(G). By Theorem 27 there exists an integer $k \geq 0$ and p in $P(E(V))$ such that $(d|_G)^k(f \circ \rho) = p|_G$. Now let $x_1, \ldots, x_n$ be a basis for $G^\circ$ over the basis field K. Let $F = K\langle t_1, \ldots, t_n\rangle$ be the field of quotients of the ring of integral power series in the variables $t_1, \ldots, t_n$. Extending d, f, $\rho$ and p canonically, we see that $(d_G F)^k(f \circ \rho^F) = p|_{G^F}$ because G is a unicity set in $G^F$.

From the proof of Theorem 1, we know that $\exp(t_i x_i)$ belongs to $G^{K\langle t_i\rangle} \subset G^F$. It follows that $\exp(t_1 x_1)\ldots\exp(t_n x_n)$ is in $G^F$. Further, $\rho^F(\exp(t_1 x_1)\ldots\exp(t_n x_n)) = \exp(t_1 \rho^\circ(x_1)\ldots\exp(t_n \rho^\circ(x_n)) = \exp(t_1\phi(x_1))\ldots\exp(t_n\phi(x_n))$. Therefore

$$(*)\quad d^k(\exp(t_1x_1)\ldots\exp(t_nx_n))f(\exp(t_1\phi(x_1))\ldots\exp(t_n\phi(x_n))) =$$

$$= p(\exp(t_1\phi(x_1))\ldots\exp(t_n\phi(x_n))) \quad .$$

From now on, let $\phi$ stand for the canonical extension of $\phi$ to $U$. Then

$$f(\exp(t_1\phi(x_1))\ldots\exp(t_n\phi(x_n)) = \exp(t_1D_{\phi(x_1)})\ldots\exp(t_nD_{\phi(x_n)})(f)(\phi(1))$$

$$= \sum \frac{1}{c_1!\ \ldots\ c_n!}\ D_\phi^{c_1}(x_1)\ldots D_\phi^{c_n}(x_n)(f)(\phi(1))t_1^{c_1}\ldots\ t_n^{c_n}$$

$$= \sum \frac{1}{c_1!\ \ldots\ c_n!}\ (f\ o\ \phi)(x_1^{c_1}\ \ldots\ x_n^{c_n})\ t_1^{c_1}\ \ldots\ t_n^{c_n} \quad .$$

Similarly,

$$p(\exp(t_1x_1)\ldots\exp(t_nx_n)) = \sum \frac{1}{c_1!\ \ldots\ c_n!}\ p'(x_1^{c_1}\ \ldots\ x_n^{c_n})t_1^{c_1}\ \ldots\ t_n^{c_n}$$

where $p'$ is the element of $R$ corresponding to $p$ via the identity representation.

$$(d^k)'(\exp(t_1x_1)\ldots\exp(t_nx_n)) =$$

$$= \sum \frac{1}{c_1!\ldots\ c_n!}\ (d^k)'(x_1^{c_1}\ \ldots\ x_n^{c_n})t_1^{c_1}\ldots\ t_n^{c_n} \quad .$$

Consider the map $R \longrightarrow K\langle t_1, \ldots, t_n\rangle$ which sends $r$ into $\sum \frac{1}{c_1!\ldots\ c_n!}\ r(x_1^{c_1}\ \ldots\ x_n^{c_n})\ t_1^{c_1}\ \ldots\ t_n^{c_n}$ . This is easily seen to be a K-algebra monomorphism and hence, (by comparing coefficients) we see that $(d')^k(f\ o\ \phi) = p'$ . Multiplying this by $z^k$ we obtain $f\ o\ \phi = z^kp'$ which is in $S[z]$. This proves the necessity of our condition.

Now suppose that $R(\phi) \subset S[z]$ . The group $G$ operates on $P(E(V))$ by left translation and leaves fixed the ideal, $\mathcal{O}$ , associated with $G$. $\mathcal{O}$ is the kernel of the homomorphism $p \longrightarrow p'$ and therefore we get an induced $G$-module structure on $S = \mathrm{Im}(p \longrightarrow p') \approx P(E(V))/\mathcal{O} \approx P(G)$.

The $G$-operations on $S$ commute with the right translations by the elements of $G^\circ$ and are also algebra automorphisms. Further, these $G$-operations extend uniquely to the field of quotients of $S$. Now $x.d = d(x)d$ for all $x$ in $G$ and therefore $x(d') = d(x)d'$ since the map $p \longrightarrow p'$ is an operator homomorphism. Also,

$$1 = x(1) = x(zd') = x(z)x(d') = x(z)d(x)d' \quad .$$

Therefore $x(z) = d(x)^{-1}z$ and hence $S[z]$ is $G$-stable.

Now $R(\phi)$ is stable under left translations by elements of $G^\circ$ and therefore it follows from Lemma 2 that $R(\phi)$ is $G$-stable. Thus we have a representation $\Psi$ of $G$ on $R(\phi)$ which commutes with the right $G^\circ$-translations. The representative functions associated with $\Psi$ are the linear combinations of the maps $x \longrightarrow x(f)(u)$ where $f$ ranges over $R(\phi)$ and $u$ ranges over $U(G^\circ)$ . Now $x(f)(u) = (x(f).u)(1) = (x(f.u))(1)$ and $f.u$ is in $R(\phi)$. Hence the representative functions associated with $\Psi$ are the maps $x \longrightarrow x(f)(1)$ . These are precisely the elements of $P(G)[\frac{1}{d}]$ corresponding to the elements of $R(G)$ under our isomorphism $P(G)[\frac{1}{d}] \approx S[z]$ induced by the map $p \longrightarrow p'$ where $\frac{1}{d} \longrightarrow z$ . Thus the representative functions associated with $\Psi$ are rational functions on $G$, i.e., $\Psi$ is a rational representation of $G$ .

Extend $\Psi$ to a rational representation of $G^{K<t>}$ in $R(\phi)\otimes_K K<t>$, still denoted by $\Psi$. For $x$ in $G^\bullet$, $\Psi(\exp tx) = \exp(t\Psi^\bullet(x))$. On the other hand, the operation with $\exp tx$ on $R(\phi)\otimes_K K<t>$ is $\exp(t\tau_x)$ where $\tau_x$ is left translation by $x$ on $R(\phi)$. In fact, it follows from the definition of the action of $\Psi$ that $\Psi(\exp(tx))(p') = \exp(tx).p)'$ for all $p$ in $P(E(V))[\frac{1}{d}]$ where $(\frac{1}{d})' = z$. Hence

$$\Psi(\exp(tx))(p') = (\exp(tD_x)(p))' = \exp(t\tau_x)(p') .$$

Let $D$ be the subspace of $R(\phi)\otimes_K M_\phi$ consisting of all $\sum_i r_i\otimes m_i$ such that $\sum_i r_i.u\otimes m_i = \sum_i r_i\otimes u.m_i$ for all $u$ in $U$. Since the G-operations on $R(\phi)$ commute with the right translations by elements of $U$, it is clear that $D$ is stable under $(\Psi\otimes 1)(G)$. Regard $R(\phi)\otimes M_\phi$ as a U-module such that for $x$ in $G^\bullet$, $x.(r\otimes m) = (x.r)\otimes m$ for all $r$ in $R(\phi)$, $m$ in $M_\phi$. Then $D$ is evidently a U-submodule of $R(\phi)\otimes M_\phi$ and the U-module structure of $D$ coincides with the U-module structure derived from the differential of our representation of $G$ on $D$, because $\Psi^\circ(x) = \tau_x$ for every $x$ in $G^\circ$. Now we claim that the U-module $D$ is isomorphic with the U-module $M_\phi$. Define the homomorphism $\alpha: D \longrightarrow M_\phi$ so that

$$\alpha(\sum_i r_i\otimes m_i) = \sum_i r_i(1)m_i .$$

Take $u$ in $U$. Then

$$\alpha(\sum_i (u.r_i)\otimes m_i) = \sum_i r_i(u)m_i = \sum_i (r_i.u)(1)m_i =$$

$$= \sum_i r_i(1)(u.m_i) = u.\alpha(\sum_i r_i\otimes m_i) .$$

Thus $\alpha$ is a U-homomorphism. Now suppose that $\sum_i r_i(1)m_i = 0$. Then also $\sum_i r_i(1)u.m_i = 0$ for every $u$ in $U$, i.e., $\sum_i (r_i.u)(1)m_i = 0$

for every $u$ in $U$, i.e., $\sum_i r_i(u)m_i = 0$ for every $u$ in $U$. We may assume that the $m_i$ are $K$-linearly independent whence $r_i = 0$ and therefore $\sum_i r_i \otimes m_i = 0$. Therefore $\alpha$ is a monomorphism.

Let $m_1, \ldots, m_p$ be a basis for $M_\phi$ and $\lambda_1, \ldots, \lambda_p$ a dual basis for $M_\phi^*$. Define $\lambda_i/m$ in $R(\phi)$ by $(\lambda_i/m)(u) = \lambda_i(um)$. We claim that $\sum_i (\lambda_i/m) \otimes m_i$ is in $D$. In fact, write $u \cdot m_j = \sum_k f_{jk}(u)m_k$. Then $(\lambda_i \circ \phi(u))(m_j) = \lambda_i(u \cdot m_j) = f_{ji}(u)$ and hence $\lambda_i \circ \phi(u) = \sum_k f_{ki}(u)\lambda_k$. Therefore $\sum (\lambda_i/m) \cdot u \otimes m_i = \sum_{i,k} f_{ki}(u)\lambda_k \otimes m_i =$

$= \sum_k \lambda_k \otimes \sum_i f_{ki}(u)m_i = \sum_k \lambda_k \otimes u \cdot m_k$ for every $u$ in $U$. Thus

$\sum_i (\lambda_i/m) \otimes m_i$ is in $D$ for every $m$ in $M_\phi$. Now $\alpha(\sum_i (\lambda_i/m) \otimes m_i) =$

$= \sum_i (\lambda_i/m)(1)m_i = \sum_i \lambda_i(m)m_i = m$. Hence $\alpha$ is an epimorphism.

We have shown that $\alpha$ is a $U$-isomorphism of $D$ onto $M_\phi$. Thus our rational representation of $G$ on $D$ is transported by $\alpha$ into a rational representation $\rho$ of $G$ on $M_\phi$ and evidently $\rho^\circ = \phi$.

Q.E.D.

University of
Connecticut
Libraries

39153027095878

BOUND BY
HM